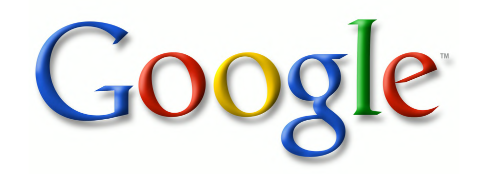
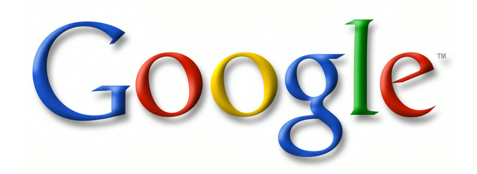




Die

unbestimmte Analytik.

Von

Dr. Hermann Scheffler.

Erste Abtheilung.

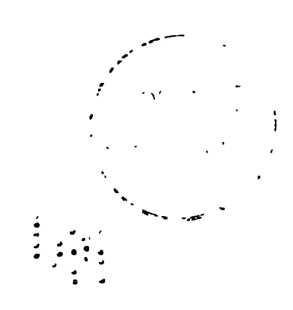
Hannover.
Im Verlage der Helwing'schen Hofbuchhandlung.
1854.

Die

unbestimmte Analytik.

Von

Dr. Hermann Scheffler.



Hannover.
Im Verlage der Helwing'schen Hofbuchhandlung.
1854.

Druck von Ph. C. Göhmann.

Vorrede.

Bekanntlich ist die unbestimmte Analytik ein neuerer Zweig der mathematischen Wissenschaften, welcher erst gegen das Ende des vorigen Jahrhunderts seine Begründung gefunden hat. Obgleich in früherer Zeit, namentlich im Alterthume von Diophant und alsdann nach einer langen Pause erst wieder in den letzten Jahrhunderten von Bachet, Fermat, Pell und Anderen, einzelne hierher gehörige Aufgaben gelös't waren; so bildeten dieselben doch durchaus kein systematisches Ganzes, welches durch einheitliche Prinzipien und allgemeine Methoden zusammengehalten und dadurch einer natürlichen Entwickelung fähig gemacht wäre. Erst Euler legte durch seine zahlreichen neuen Entdeckungen und durch das damit verbundene Streben nach allgemeinen Regeln den Grund zu dem neuen Gebäude, und Lagrange war der Erste, welcher dasselbe als ein geordnetes System in den Zusätzen zu seiner Übersetzung von Euler's Algebra aufrichtete. Diese Zusätze existiren in der deutschen Übersetzung von Kausler aus dem Jahre 1796 als ein für sich bestehendes Werk. Hierin gibt Lagrange ausser der von Euler erfundenen Methode eine neue auf die Theorie der Kettenbrüche gestützte und früher schon von Bachet angedeutete Methode zur Auflösung der unbestimmten Gleichungen vom ersten Grade; ausserdem lehrt er die unbestimmten Gleichungen vom zweiten Grade mit zwei Unbekannten auflösen, wobei er die Gleichungen nach drei Klassen unterscheidet: solche mit positiver, negativer und quadratischer

Determinante. Jede Klasse wird nach einer besonderen Methode behandelt; die Methoden für die ersten beiden Klassen stützen sich auf die Kettenbrüche, die für die dritte Klasse jedoch nicht.

So gross hiernach Lagrange's Verdienst um die unbestimmte Analytik, namentlich wegen der Ausdehnung seiner Untersuchungen auf die Gleichungen vom zweiten Grade ist; so lässt seine Auflösung doch noch Manches in Hinsicht auf Allgemeinheit, Eleganz und Kürze zu wünschen übrig. Denn theils kann diese Auflösung, wie schon bemerkt, nicht in allen Fällen nach Ein und derselben Regel bewirkt werden, sondern erfordert je nach den Umständen bald die Eine, bald die andere von drei ganz verschiedenen Methoden; das Auflösungsverfahren enthält also eine Spaltung der Prinzipien, welche um so mehr befremdet, als sie bei der Behandlung der bestimmten Gleichungen nicht vorkommt. Ausserdem besitzt diese Auflösung der unbestimmten quadratischen Gleichungen nicht den wünschenswerthen Grad von Eleganz und erweis't sich etwas schwerfällig bei ihrer Ausführung, besonders, wenn man darauf ausgeht, die Reihen der möglichen Werthe der Unbekannten innerhalb gewisser Werthe vollständig zu ermitteln, was in den meisten Fällen ein Bedürfniss ist.

Ferner lös't Lagrange in der erwähnten Schrift die homogenen Gleichungen vom zweiten Grade mit drei Unbekannten auf. Diese Auflösung ist ebenfalls neu und geistreich, jedoch mit ähnlichen Mängeln für den praktischen Gebrauch behaftet, wie die vorhergehende.

Auf diese Arbeit von Lagrange gestützt, gab Legendre im Jahre 1799 seine *Essais sur la théorie des nombres* heraus. In diesem Werke finden sich für die Auflösungen der unbestimmten Gleichungen vom ersten und zweiten Grade die Methoden von Lagrange reproduzirt und nur durch verschiedene Zusätze und Ausführungen weiter entwickelt, weshalb sich im Wesentlichen davon das Frühere sagen lässt.

Ausserdem aber hat Legendre in dem letzteren Werke die Untersuchungen auf ein eigenthümliches Gebiet der

Zahlenlehre geleitet, in welchem vornehmlich die Gesetze der ganzen Zahlen untersucht werden und welches nach ihm die Theorie der Zahlen genannt ist. Diese Theorie erscheint in Legendre's Werke noch als eine Sammlung isolirter Sätze ohne methodischen Zusammenhalt. Es waren also noch die allgemeinen Prinzipien zu erfinden, wodurch jene zerstreuten Wahrheiten zu einem natürlichen Systeme vereinigt und weiter ausgebildet werden konnten.

Diese Prinzipien waren allerdings schon erfunden, wurden aber erst im Jahre 1801 durch das höchst originelle Werk von Gauss, *Disquisitiones arithmeticae*, bekannt gemacht. Hierin entwickelt der berühmte Verfasser, gestützt auf die von ihm erfundene Lehre von der Kongruenz der Zahlen, nicht bloss in viel vollkommenerem Grade diejenigen Wahrheiten, welche den eigentlichen Gegenstand der Theorie der Zahlen ausmachen, sondern wendet jene Lehre vorzugsweise auf die Umformung der Formeln an, wovon in letzter Instanz die Auflösung der unbestimmten Gleichungen vom zweiten Grade abhängt. Die Durchführung des letzteren Gegenstandes, nämlich die Umformung und Auflösung der unbestimmten quadratischen Gleichungen, ist schön und bewunderungswürdig wegen des Ideenreichthums und der vielen daraus sich ergebenden interessanten Wahrheiten; es ist auch nicht zu bezweifeln, dass zu gewissen Zwecken die Gauss'schen Transformationsmethoden das vorzüglichste Hülfsmittel darbieten: allein zu dem besonderen Zwecke der Auflösung jener Gleichungen erscheint der Rechenaufwand, welchen sie erfordern, als zu erheblich, um den Anforderungen der Praxis vollständig zu entsprechen.

Die Methode von Gauss, soweit sie sich auf die allgemeinen quadratischen Gleichungen mit zwei und die homogenen quadratischen Gleichungen mit drei Unbekannten bezieht, ist von einem allgemeineren Standpunkte aufgefasst, als die von Lagrange, aber deshalb auch komplizirter und schwieriger. Jener allgemeinere Standpunkt verstattet der Methode von Gauss ein weiteres Vordringen in diesem Gebiete, und zunächst in die Theorie

der allgemeinen quadratischen Gleichungen mit drei Unbekannten. Die Auflösung der Letzteren ist jedoch von Gauss nur angebahnt, noch nicht bewirkt.

Seit dem Erscheinen der genannten Werke von Lagrange, Legendre und Gauss ist die Litteratur der Lehrbücher über den fraglichen Gegenstand äusserst dürftig geblieben. Mit Ausnahme eines kleinen Werkes von Minding über die Anfangsgründe der höheren Arithmetik, durch welches der Leser mit den Grundprinzipien der zuerst genannten drei Werke in gedrängter Kürze bekannt gemacht wird, dürfte die neuere Litteratur ein bemerkenswerthes Kompendium der fraglichen Lehren überall nicht aufzuweisen haben. Ja, das mathematische Wörterbuch von Klügel liefert sogar unter dem Artikel der unbestimmten Analytik, soweit derselbe sich auf die Gleichungen vom zweiten Grade bezieht, einen fast wörtlichen, aber dabei doch so unvollständigen Auszug aus dem oben erwähnten ältesten Werke von Lagrange, dass danach die Auflösung der Gleichung $ax^2+2bxy+cy^2=k$, wenn die Determinante positiv und kein Quadrat ist, im Allgemeinen gar nicht bewirkt werden kann. Wenn man hin und wieder durch das in jenem Artikel angedeutete Verfahren wirklich eine Reihe von Auflösungen erhält; so beruhet Dies auf einer zufälligen, nicht einmal näher charakterisirten Beschaffenheit der Koeffizienten der gegebenen Gleichung: gleichwol darf man auch in einem solchen speziellen Falle nicht erwarten, dass die angezeigte Methode alle möglichen, sondern nur eine gewisse Reihe von Auflösungen ergebe.

Allerdings haben viele der ausgezeichnetsten neueren Mathematiker, insbesondere Seeber, Lejeune-Dirichlet, Jacobi, Eisenstein, Kummer, Crelle, Arndt, Hermite, Libri und Andere, der unbestimmten Analytik eine bedeutende Aufmerksamkeit geschenkt; aber vorzugsweise sind ihre Bemühungen darauf gerichtet gewesen, in einzelnen Abhandlungen gewisse Theile der Theorie von Gauss weiter auszubilden und die höheren Probleme der unbestimmten Analytik zu lösen. Unter solchen Umständen, wo

wenig Anstrengungen gemacht sind, um durch Vereinfachung der Grundoperationen die Schwierigkeiten des Kalkuls zu beseitigen und durch Bearbeitung von Lehrbüchern den Gegenstand populär zu machen, ist der Zugang zu diesem wichtigen und interessanten Theile der Mathematik dem grösseren Publikum, welches einer mathematischen Bildung bedarf, bis jetzt völlig verschlossen geblieben, und Dies um so mehr, da die meisten Lehrbücher der allgemeinen Arithmetik von den unbestimmten Aufgaben noch nicht einmal die Elemente enthalten.

Es ist daher die Tendenz des vorliegenden Werkes, den fraglichen Lehren einen weiteren Leserkreis zu gewinnen, mit Ausschluss der transzendenteren Theile, welche das gewöhnliche Bedürfniss weit überragen und in der That jetzt durchaus noch nicht in sich abgeschlossen sind, den Grundstoff der Wissenschaft in einer leicht fasslichen, für die praktische Anwendung besonders eingerichteten Weise zu behandeln, für die komplizirteren Methoden bequeme Regeln zu entwickeln und die Ausführung durch eine genügende Zahl angemessener Beispiele, welche sich in den bisherigen Schriften nur sehr spärlich finden, obgleich sie zur Illustrirung dieses Kalkuls äusserst nöthig sind, zu erläutern. Dabei hat sich die Gelegenheit dargeboten, manches Neue mitzutheilen und für manche Gesetze eigenthümliche Gesichtspunkte zu gewinnen, sodass das Ganze auch für das höhere mathematische Publikum nicht ohne Interesse sein dürfte. Im Speziellen ist über den Inhalt Folgendes zu bemerken.

Der erste Abschnitt enthält die Theorie der endlichen Kettenbrüche. Diese Theorie ist schon an sich und wegen ihrer anderweiten vielfachen Anwendungen in der Mathematik wichtig und findet sich fast in allen Lehrbüchern der Arithmetik ungenügend entwickelt. Hier bildet sie ausserdem die Basis für die unbestimmte Analytik und enthält manche Eigenthümlichkeit und Erweiterung gegen die bisherigen Darstellungen.

Der zweite Abschnitt enthält die Auflösung der unbestimmten Gleichungen vom ersten Grade mit

beliebig vielen Unbekannten. §. 28 lehrt das Grundverfahren von Euler und §. 30 das von Lagrange. Das Letztere ist jedoch in mehrfacher Hinsicht verallgemeinert. Für den allgemeinsten Fall von mehreren Gleichungen mit mehreren Unbekannten ist in §. 39 ein einfaches und alle Spezialitäten umfassendes Verfahren mitgetheilt.

Der dritte Abschnitt enthält die sehr wichtige und bis jetzt nur unvollständig bearbeitete Theorie der Ungleichheiten vom ersten Grade, welche für die unbestimmte Analytik wegen der Bestimmung der Gränzen der Willkürlichen nach gegebenen Bedingungen von besonderer Bedeutung ist, ausserdem aber, wie in §. 56 ff. gezeigt ist, die Elemente zur Auflösung einer eigenthümlichen Klasse von Aufgaben enthält. Diese Theorie ist in §. 42 ff. und in §. 50 ff. nach zwei verschiedenen Methoden entwickelt.

Der vierte Abschnitt enthält die Theorie der unendlichen periodischen Kettenbrüche, wie sie aus der Entwickelung der quadratischen Irrationalgrösse von der Form $\frac{\sqrt{D}+P}{Q}$ hervorgehen. Diese Lehren haben schon an sich ein bedeutendes Interesse; hier liefern sie aber noch den Schlüssel zu einem äusserst praktischen und allgemein gültigen Verfahren behuf Auflösung der unbestimmten Gleichungen vom zweiten Grade. Zu dem Ende wird das der Entwickelung der irrationalen Grösse $\frac{\sqrt{D}+P}{Q}$ in einen Kettenbruch zu Grunde liegende Prinzip in §. 87 ff. auch auf den Fall ausgedehnt, wo die Determinante D ein Quadrat ist, ferner in §. 93 ff. auf den Fall, wo D gleich null ist, und endlich in §. 94 ff. auf den Fall, wo D negativ ist.

Der fünfte Abschnitt enthält die Auflösung der unbestimmten Gleichungen vom zweiten Grade mit zwei Unbekannten in ganzen Zahlen und die wichtigsten Betrachtungen über quadratische Formen.

Die Auflösungsmethode der Gleichungen von der Form $ax^2+bxy+cy^2=k$ in §. 100 ist völlig allgemein und von dem Werthe der Determinante ganz unabhängig.

Dieselbe unterscheidet sich daher wesentlich von den Methoden von Lagrange und von Gauss. Dass dieselbe zugleich bedeutend einfacher und viel leichter auszuführen ist, besonders, wenn man die verschiedenen Reihen der Werthe von x und y innerhalb gewisser Gränzen vollständig zu ermitteln hat, dürfte mit Evidenz aus den zahlreichen Beispielen der folgenden Paragraphen hervorgehen.

Für den Fall, wo die Determinante gleich null ist, umschliesst das vorstehende Verfahren zugleich die Auflösung der unbestimmten Gleichungen vom ersten Grade, was in §. 114 näher erläutert ist.

Da sich die Fälle, wo die Determinante ein Quadrat, oder null, oder negativ ist, zuweilen leichter nach anderen Methoden behandeln lassen; so sind die desfallsigen Regeln in §. 121 und 122 besonders mitgetheilt.

Die in §. 100 entwickelte Auflösungsmethode für den allgemeineren Fall, wo die Determinante positiv und kein Quadrat, die Anzahl der Werthe von x und y also stets unendlich ist, beruhet auf einem gewissen Rekursionsprinzipe. In §. 123 sind aber auch independente Formeln für x und y mitgetheilt.

Nach §. 124 lässt sich die für die Gauss'sche Theorie so wichtige, für unsere Zwecke aber weniger erhebliche Transformation und Reduktion der quadratischen Formen mit mechanischer Leichtigkeit ausführen, auch die Äquivalenz derselben ohne Mühe konstatiren, wie denn überhaupt dieser Paragraph die Elemente zu einer selbstständigen Entwickelung der Theorie der quadratischen Formen darbietet.

§. 125 ff. lehren die allgemeinen quadratischen Gleichungen mit zwei Unbekannten von der Form $ax^2 + bxy + cy^2 + dx + ey = k$ rekursorisch auflösen und §. 127 gibt die independenten Formeln auch für diese Gattung von Gleichungen.

Der sechste Abschnitt enthält die Kongruenz der Zahlen und das damit Verwandte, was den eigentlichen Gegenstand der Theorie der Zahlen ausmacht,

innerhalb derjenigen Gränzen, welche der Bestimmung des Buches zu entsprechen schienen. Man wird auch hier manches Neue und Eigenthümliche, namentlich aber möglichste Einfachheit der Beweise und Entwickelungen antreffen.

Der siebente Abschnitt enthält die Auflösung der homogenen quadratischen Gleichungen mit drei Unbekannten in ganzen Zahlen und die der allgemeinen Gleichungen mit zwei Unbekannten in rationalen Zahlen.

Die Methode in §. 161 zur Auflösung der Gleichung von der Form $x^2 = by^2 + cz^2$, auf welche in §. 172 die der allgemeineren Gleichung $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$ zurückgeführt wird, gründet sich auf das von Lagrange angegebene Verfahren, ist jedoch bedeutend einfacher und systematischer als das letztere, was in §. 166 an einem auch von Lagrange berechneten Beispiele evident gemacht ist. In §. 167 ist das Auflösungsverfahren in wissenschaftlicher Beziehung noch weiter vervollkommnet, wenngleich bei der praktischen Behandlung von dieser Modifikation abgesehen werden kann.

Der achte Abschnitt ist der Auflösung der homogenen quadratischen Gleichungen mit beliebig vielen Unbekannten in ganzen Zahlen und der allgemeinen Gleichungen mit beliebig vielen Unbekannten in rationalen Zahlen gewidmet.

Wenngleich durch diesen Abschnitt das Problem nicht in seiner ganzen Allgemeinheit gelös't worden; so ist dadurch das Gebiet der unbestimmten Analytik doch erweitert. Dies ist durch ganz elementare, den früheren Methoden analoge Mittel geschehen, welche bei gehöriger Ausbildung gewiss geeignet sein werden, zum Zweck der Auflösung dieser Gleichungen die äusserst schwierigen und mühsamen Gauss'schen Transformationen zu ersetzen, welche Letzteren trotz der Anstrengungen eines Gauss, Seeber, Eisenstein u. A. bis jetzt noch nicht einmal zur vollständigen Auflösung der quadratischen Gleichungen mit drei Unbekannten, deren linke Seite homogen ist, geführt haben;

und welche, auch wenn sie dieses Ziel endlich einmal erreichen sollten, für die praktische Anwendung zu komplizirt bleiben möchten.

Im Übrigen lässt sich leicht zeigen, dass sich das in dieser Schrift fast durchgängig in Anwendung gebrachte Entwickelungsprinzip mittelst der Kettenbrüche mit dem Gauss'schen Verfahren zu grosser Vereinfachung des Letzteren dergestalt verbinden lässt, dass die schwierigen Transformationen der ternären Formen, der Übergang zu den adjungirten Formen und die Substitutionen, welche ein Durchlaufen ganzer Reihen äquivalenter Formen zum Zwecke haben, auf einfache Kettenbruchsentwickelungen und mechanische Umgestaltung der Formeln zurückgeführt werden. Die nähere Ausführung der desfallsigen Operationen ist in gegenwärtiger Schrift unterblieben, weil sich dieselbe hierdurch zu weit von ihrer nächsten Bestimmung entfernt hätte, und der höhere Mathematiker, welcher hierauf einzugehen beabsichtigen sollte, die desfallsigen Beziehungen leicht selbst ermitteln wird.

Der neunte Abschnitt enthält die endlichen Kettenbrüche, die Auflösung der unbestimmten Gleichungen vom ersten Grade und verwandte Gegenstände, welche in den ersten drei Abschnitten unter der Voraussetzung reeller Zahlen behandelt worden, unter der allgemeinsten Voraussetzung **komplexer** Zahlen.

Der Inhalt dieses Abschnittes wird, wennauch nicht immer auf Neuheit, doch durchgehends auf Eigenthümlichkeit der Entwickelung Anspruch machen können, indem ich die in diesem und dem folgenden Abschnitte enthaltenen Sätze über die komplexen Zahlen schon zu einer Zeit aufgefunden hatte, als mir die ersten Untersuchungen über diesen Gegenstand von Gauss in dessen *Theoria residuorum biquadraticorum*, sowie die von Lejeune-Dirichlet, Eisenstein u. A. in dem Crelle'schen Journale noch ganz unbekannt waren.

Die Entwickelung eines rationalen Bruches mit komplexem Zähler und Nenner in einen Kettenbruch §. 196 und die Beziehungen zwischen den Näherungswerthen

eines solchen Kettenbruches §. 197 ff. führt zu sehr beachtenswerthen Gesetzen. Diese Gesetze werden aber besonders durch ihre geometrische Bedeutung interessant. Die Beziehung zwischen der komplexen Zahlform und der Geometrie ist die Basis einer besonderen analytischen Behandlungsweise der Geometrie geworden, welche ich in einem kürzlich erschienenen Buche unter dem Namen Situationskalkul ausführlich entwickelt und praktisch verwendbar gemacht habe. Die Prinzipien des Situationskalkuls spielen auch in den letzten beiden Abschnitten der gegenwärtigen Schrift eine wichtige Rolle, da sie die bei rein arithmetischer Auffassung oftmals höchst verwickelten Gesetze durch geometrische Darstellung ungemein anschaulich machen und ausserdem zeigen, wie sich die meistens nur auf stetige Grössenbildungen angewandte Geometrie mit grossem Vortheile auch zu Entdeckungen auf dem Gebiete der diskreten ganzen Zahlen verwenden lässt, was bisher gewiss nur selten und ohne erheblichen Erfolg versucht sein möchte.

Der zehnte Abschnitt verallgemeinert für komplexe Zahlen diejenigen Untersuchungen, welche den Gegenstand des vierten bis achten Abschnittes ausmachen und worin die Formen vom zweiten Grade die Hauptrolle spielen. Demnach sind darin die unendlichen periodischen Kettenbrüche, die unbestimmten quadratischen Gleichungen und die wichtigsten Sätze der Kongruenz der Zahlen in der schon bei dem vorhergehenden Abschnitte bemerkten selbstständigen Entwickelungsweise behandelt worden.

Schliesslich wird bemerkt, dass es für angemessen gehalten ist, aus den ersten fünf Abschnitten, welche den elementareren Theil umfassen und innerhalb der gewöhnlichen Gränzen des Lehrplans höherer Unterrichtsanstalten liegen, eine besondere und für sich verkäufliche Abtheilung dieses Werkes zu bilden.

Braunschweig im September 1853.

H. Scheffler.

Inhalt.

Erster Abschnitt.

Endliche Kettenbrüche.

Zweiter Abschnitt.

Auflösung der unbestimmten Gleichungen vom ersten Grade in ganzen Zahlen.

Dritter Abschnitt.

Theorie der Ungleichheiten vom ersten Grade.

Erste Auflösungsmethode.

Zweite Auflösungsmethode, durch Zurückführung der Ungleichheiten auf Gleichungen mit begränzt Veränderlichen.

Vierter Abschnitt.

Unendliche periodische Kettenbrüche.

Entwickelung irrationaler reeller Quadratwurzeln in Kettenbrüche.

Sechster Abschnitt.

Die Kongruenz der Zahlen.

Siebenter Abschnitt.

Auflösung 1) der homogenen Gleichungen vom zweiten Grade mit drei Unbekannten sowol in ganzen, wie in rationalen Zahlen und 2) der allgemeinen Gleichungen vom zweiten Grade mit zwei Unbekannten in rationalen Zahlen.

Homogene Gleichungen mit drei Unbekannten in ganzen Zahlen.

Homogene Gleichungen in rationalen Zahlen.

Allgemeine Gleichungen mit zwei Unbekannten in rationalen Zahlen.

Achter Abschnitt.

Allgemeine Gleichungen vom zweiten Grade mit drei und mehr Unbekannten.

Homogene Gleichungen mit vier Unbekannten in ganzen Zahlen.

Homogene Gleichungen mit beliebig vielen Unbekannten in ganzen Zahlen.

Allgemeine Gleichungen mit drei oder mehr Unbekannten in rationalen Zahlen.

Neunter Abschnitt.

Komplexe Zahlen und die daraus gebildeten Kettenbrüche und unbestimmten Gleichungen vom ersten Grade.

Zehnter Abschnitt.

Unendliche Kettenbrüche, unbestimmte Gleichungen vom zweiten Grade und Grundlehren der Kongruenz in komplexen Zahlen.

Druckfehler.

Seite	17	Zeile	3	von oben statt N_0 lies N
„	68	„	10	„ „ „ b „ 6
„	96	„	13	„ „ „ $240w$, lies $240,w$
„	110	„	13	„ „ „ w_2 lies w_1
„	158	„	7	„ „ hinter dem Worte bestätigt lies: Jede zweigliederige Periode ist also auch symmetrisch
„	206	„	9	„ „ statt 155 lies 150
„	231	„	13	von unten statt a_0 lies a_n
„	238	„	13	von oben statt Fluss lies Schluss
„	260	„	7	von unten statt ± 1, lies $\pm 1)$
„	316	„	5	von oben statt negativ lies relativ
„	345	„	2	und 3 von unten statt eingliederige lies viergliederige
„	350	„	3	von unten statt h^{m-2}, h^{m-4}, h^{m-6} lies H^{m-2}, H^{m-4}, H^{m-6}
„	359	„	15	von unten statt der lies die
„	384	„	5	von unten statt $2a$ lies $3a$
„	566	„	2	von oben statt $p=qi$ lies $p+qi$
„	576	„	11	von unten statt bi lies $6i$
„	622	„	14	von unten statt $2q$ lies $2(q$

Erster Abschnitt.

Endliche Kettenbrüche.

§. 1. *Allgemeine Begriffe.*

Nennen wir den zweigliederigen Ausdruck $a \pm \frac{b}{c}$, dessen zweites Glied in Form eines Bruches dargestellt ist, eine gemischte Zahl und c den Nenner derselben; so entsteht ein Kettenbruch oder kontinuirlicher Bruch dadurch, dass man den Nenner einer gemischten Zahl wiederum als gemischte Zahl erscheinen lässt und dasselbe Bildungsgesetz beliebig viel Mal immer auf den Nenner der zuletzt entstehenden gemischten Zahl in Anwendung bringt. Ein Kettenbruch hat also die allgemeine Form

$$a \pm \cfrac{b}{c \pm \cfrac{d}{e \pm \cfrac{f}{g \pm \text{etc.}}}}$$

Bricht dieses Bildungsgesetz nach einer endlichen Menge von Wiederholungen ab, so entsteht ein endlicher, im entgegengesetzten Falle ein unendlicher Kettenbruch. Wir haben es in diesem Abschnitte nur mit den ersteren zu thun.

Die Zahlen $a, c, e, g \ldots$ heissen die Quotienten des Kettenbruchs.

Wir werden in dieser Schrift nur solche Kettenbrüche betrachten, in welchen die Zähler $b, d, f \ldots$ sämmtlich $= 1$ und die Quotienten $a, c, e, g \ldots$ sämmtlich ganze Zahlen sind.

Wenn alle Quotienten positiv und mit Ausnahme des ersten a, welcher auch $= 0$ sein kann, > 0 sind, und wenn ausserdem die beiden Theile aller Nenner nur durch Addition verbunden sind; so ergibt sich ein gewöhnlicher oder gemeiner

Kettenbruch, mit welchem wir uns zunächst beschäftigen wollen. Einen solchen in der Form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \text{etc.}}}}$$

enthaltenen Kettenbruch werden wir kurz mit

$$[a_0, a_1, a_2, a_3 \ldots]$$

bezeichnen.

Hiernach ist z. B.

$$3 + \cfrac{1}{5 + \cfrac{1}{7}} = [3, 5, 7] \quad , \quad \cfrac{1}{5 + \cfrac{1}{7}} = [0, 5, 7]$$

Der Erfinder der Kettenbrüche soll Brounker sein.

§. 2. *Reduktion eines Kettenbruchs auf einen gemeinen Bruch von unten nach oben.*

Der Werth eines jeden Kettenbruchs von der Form $\cfrac{1}{a_1 + \cfrac{1}{a_2 + \text{etc.}}}$ ist >0 und <1, indem offenbar der Werth x von $a_1 + \cfrac{1}{a_2 + \text{etc.}} > 1$, also der fragliche Kettenbruch $\frac{1}{a_1 + x} > 0$ und <1 ist. Nur wenn alle späteren Quotienten von a_2 an nicht vorhanden und $a_1 = 1$ wäre, würde der gegebene Kettenbruch $\frac{1}{a_1} = 1$ sein, ein Fall, der übrigens nicht leicht vorkommen kann, weil der Kettenbruch $0 + \frac{1}{1}$ in der Form $a_0 = 1$ enthalten ist.

Hieraus folgt, dass der Werth eines Kettenbruchs von der Form $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \text{etc.}}} > a_0$ und $< a_0 + 1$ ist. Demnach nennt man den obersten Quotienten a_0 die Ganzen des Kettenbruchs.

Die Verwandlung eines Kettenbruchs in einen gemeinen Bruch oder die Reduktion eines Kettenbruchs beruhet auf der wiederholten Anwendung der Formel $a + \frac{b}{c} = \frac{ac + b}{c}$. Lässt man die Reduction von unten nach oben fortschreiten; so hat man noch die Formel $\cfrac{1}{\cfrac{a}{b}} = \frac{b}{a}$.

abwechselnd mit der vorstehenden anzuwenden, und es ergibt sich z. B. für den Kettenbruch $K = 3 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{7}}}$ folgende

Rechnung: $2 + \frac{1}{7} = \frac{15}{7}$ also $K = 3 + \cfrac{1}{5 + \cfrac{1}{\frac{15}{7}}} = 3 + \cfrac{1}{5 + \frac{7}{15}}$

ferner $5 + \frac{7}{15} = \frac{82}{15}$ also $K = 3 + \cfrac{1}{\frac{82}{15}} = 3 + \frac{15}{82}$

endlich $3 + \frac{15}{82} = \frac{261}{82} = K$.

§. 3. *Reduktion eines Kettenbruchs von oben nach unten durch Rekursion. — Näherungsbrüche.*

I. Bequemer und fruchtbarer für spätere Untersuchungen, auch anwendbar auf die unendlichen Kettenbrüche, ist das Reduktionsverfahren, welches von oben nach unten fortschreitet. Der Gesammtwerth des Kettenbruchs $[a_0, a_1, a_2 \ldots a_r]$ sei $= K$. Denken wir uns denselben nach und nach erst unmittelbar hinter dem Quotienten a_0, dann hinter a_1, dann hinter a_2 u. s. w. abgebrochen; so sei
$K_0 = [a_0]$, $K_1 = [a_0, a_1]$, $K_2 = [a_0, a_1, a_2]$ u. s. w., endlich $K_r = [a_0, a_1, a_2 \ldots a_r] = K$.

Nachdem die Werthe von $K_0, K_1, K_2 \ldots K_r$ durch das sofort zu beschreibende Verfahren als gemeine Brüche dargestellt sein werden, seien resp. $M_0, M_1, M_2 \ldots M_r$ deren Zähler und $N_0, N_1, N_2 \ldots N_r$ deren Nenner, indem wir den letzten Zähler M_r auch $= M$ und den letzten Nenner N_r auch $= N$ setzen, so dass man hat

$$K_0 = \frac{M_0}{N_0},\ K_1 = \frac{M_1}{N_1} \ldots K_r = \frac{M_r}{N_r} = K = \frac{M}{N}.$$

Ausserdem werde der Werth der hinter irgend einem Quotienten a_n folgenden Grösse, welche selbst ein Kettenbruch von der Form $\cfrac{1}{a_{n+1} + \cfrac{1}{a_{n+2} + \text{etc.}}}$ ist, mit x_n bezeichnet. Für $n = r$ hat man $x_r = 0$. Zwei benachbarte Werthe von x stehen in der Beziehung $x_n = \frac{1}{a_{n+1} + x_{n+1}}$.

Hiernach kann der Werth von K in folgende verschiedene Formen gebracht werden

$$K = a_0 + x_0 = a_0 + \cfrac{1}{a_1 + x_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + x_2}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + x_3}}} \text{ u. s. w.}$$

II. Es ist klar, dass wenn man den Werth von K_n mit Hülfe der Quotienten $a_0, a_1 \ldots a_n$ dargestellt hat, man sofort den Werth von K erhält, wenn man darin für a_n den Werth $a_n + x_n$ setzt, auch dass wenn man den Werth von K mit Hülfe der Quotienten $a_0, a_1 \ldots a_n$ und der Grösse x_n dargestellt hat, man daraus den Werth von K_n erhält, wenn man $x_n = 0$ setzt, endlich dass man aus dem letzteren Werthe von K einen neuen Werth für dieselbe Grösse erhält, wenn man darin $x_n = \frac{1}{a_{n+1} + x_{n+1}}$ setzt.

Nun hat man zuvörderst $K = a_0 + x_0$, also für $x_0 = 0$ $K_0 = a_0$ d. i. $\frac{M_0}{N_0} = \frac{a_0}{1}$, folglich $M_0 = a_0$ und $N_0 = 1$, mithin $K = \frac{M_0 + 1 . x_0}{N_0 + 0 . x_0}$.

Ferner hat man, wenn in dem letzteren Werthe von K $x_0 = \frac{1}{a_1 + x_1}$ gesetzt wird,

$$K = \frac{M_0 + \frac{1}{a_1 + x_1}}{N_0} = \frac{a_1 M_0 + 1 + M_0 x_1}{a_1 N_0 + N_0 x_1},$$

also für $x_1 = 0$ $K_1 = \frac{M_1}{N_1} = \frac{a_1 M_0 + 1}{a_1 N_0}$, folglich $M_1 = a_1 M_0 + 1$ und $N_1 = a_1 N_0$, mithin $K = \frac{M_1 + M_0 x_1}{N_1 + N_0 x_1}$.

Ferner hat man, wenn in dem letzteren Werthe von K $x_1 = \frac{1}{a_2 + x_2}$ gesetzt wird,

$$K = \frac{M_1 + \frac{M_0}{a_2 + x_2}}{N_1 + \frac{N_0}{a_2 + x_2}} = \frac{a_2 M_1 + M_0 + M_1 x_2}{a_2 N_1 + N_0 + N_1 x_2},$$

also für $x_2 = 0$ $K_2 = \frac{M_2}{N_2} = \frac{a_2 M_1 + M_0}{a_2 N_1 + N_0}$, folglich $M_2 = a_2 M_1 + M_0$ und $N_2 = a_2 N_1 + N_0$, mithin $K = \frac{M_2 + M_1 x_2}{N_2 + N_1 x_2}$.

III. Aus diesen Entwickelungen entnehmen wir das allgemeine Gesetz, wonach sich irgend ein späterer Zähler M_n und Nenner N_n aus dem Quotienten a_n und den beiden zunächst vorhergehenden Zählern M_{n-1}, M_{n-2} und Nennern N_{n-1}, N_{n-2} durch die Formeln

$$1)\quad M_n = a_n\, M_{n-1} + M_{n-2} \qquad N_n = a_n\, N_{n-1} + N_{n-2}$$

bilden lässt, und wonach auch

$$2)\quad K = \frac{M_n + M_{n-1}\, x_n}{N_n + N_{n-1}\, x_n}$$

ist, und beweisen dasselbe folgendermaassen.

Angenommen, für irgend einen Zeiger oder Index n sei die Richtigkeit dieses Gesetzes dargethan, man habe also $K = \frac{M_n + M_{n-1}\, x_n}{N_n + N_{n-1}\, x_n}$. Setzt man hierin $x_n = \frac{1}{a_{n+1} + x_{n+1}}$; so kommt nach gehöriger Reduktion $K = \frac{a_{n+1}\, M_n + M_{n-1} + M_n\, x_{n+1}}{a_{n+1} N_n + N_{n-1} + N_n\, x_{n+1}}$,

also für $x_{n+1} = 0$ $\quad K_{n+1} = \frac{a_{n+1}\, M_n + M_{n-1}}{a_{n+1}\, N_n + N_{n-1}}$, mithin

$$M_{n+1} = a_{n+1}\, M_n + M_{n-1} \qquad N_{n+1} = a_{n+1}\, N_n + N_{n-1}$$

und $\quad K = \frac{M_{n+1} + M_n\, x_{n+1}}{N_{n+1} + N_n x_{n+1}}$.

Wenn also das obige Gesetz für den Zeiger n gilt; so gilt es auch für den Zeiger $n+1$. Da dasselbe aber vorhin für $n = 2$ nachgewiesen ist; so hat es eine allgemeine Gültigkeit.

IV. Die vorstehenden Formeln, nach welchen man aus zwei benachbarten Werthen K_{n-2} und K_{n-1} und dem Quotienten a_n den nächstfolgenden Werth K_n berechnen kann, sind Rekursionsformeln, und können unbedingt vom Zeiger $n = 2$ an in Anwendung gebracht werden. Da man aber die Grössen von den vorgehenden Zeigern 0 und 1 in folgende Formen

$$M_0 = a_0 = a_0\,.\,1 + 0 \qquad N_0 = 1 = a_0 .0 + 1$$
$$M_1 = \qquad a_1 M_0 + 1 \qquad N_1 = a_1 N_0 = a_1 N_0 + 0$$

bringen kann; so leuchtet ein, dass das obige Gesetz sogar schon von dem Zeiger $n = 0$ an gültig ist, wenn man des Systems wegen Grössen von den Zeigern -1 und -2 fingirt, für welche

$$M_{-2} = 0 \qquad N_{-2} = 1$$
$$M_{-1} = 1 \qquad N_{-1} = 0$$

ist. Alsdann hat man

$$M_0 = a_0\; M_{-1} + M_{-2} \qquad N_0 = a_0\; N_{-1} + N_{-2}$$
$$M_1 = a_1\; M_0 + M_{-1} \qquad N_1 = a_1\; N_0 + N_{-1}$$
$$M_2 = a_2\; M_1 + M_0 \qquad N_2 = a_2\; N_1 + N_0$$

$$M_3 = a_3\, M_2 + M_1 \qquad N_3 = a_3\, N_2 + N_1$$

$$\vdots \qquad\qquad \vdots$$

$$M_n = a_n\, M_{n-1} + M_{n-2} \qquad N_n = a_n\, N_{n-1} + N_{n-2}$$

$$\vdots \qquad\qquad \vdots$$

$$M = M_r = a_r\, M_{r-1} + M_{r-2} \qquad N = N_r = a_r\, N_{r-1} + N_{r-2}$$

V. Hiernach kann man die Berechnung der vorstehenden Grössen stets sehr bequem nach folgendem Schema ausführen

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	a_0	$a_0\, M_{-1} + M_{-2}$	$a_0\, N_{-1} + N_{-2}$
1	a_1	$a_1\, M_0 + M_{-1}$	$a_1\, N_0 + N_{-1}$
2	a_2	$a_2\, M_1 + M_0$	$a_2\, N_1 + N_0$
4	a_3	$a_3\, M_2 + M_1$	$a_3\, N_2 + N_1$
.	.	.	.
.	.	.	.
.	.	.	.
r	a_r	$a_r\, M_{r-1} + M_{r-2}$	$a_r\, N_{r-1} + N_{r-2}$

So hat man z. B. für den Kettenbruch [3, 2, 5, 1, 4, 7]

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	3	3	1
1	2	7	2
2	5	38	11
3	1	45	13
4	4	218	63
5	7	1571	454

also $K = K_5 = \frac{1571}{454}$

Für einen Kettenbruch, dessen oberster Quotient $a_0 = 0$ ist, hat man genau dieselbe Rechnung. Z. B. für [0, 2, 5, 1, 4, 7]

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	2	1	2
2	5	5	11
3	1	6	13
4	4	29	63
5	7	209	454

also $K = K_5 = \frac{209}{454}$

VI. Die Grössen K_{-2}, K_{-1}, K_0, K_1 . . . K_{r-1}, deren Zähler und Nenner soeben bestimmt sind, heissen aus einem weiter unten nachzuweisenden Grunde die Näherungswerthe oder Näherungsbrüche des gegebenen Kettenbruchs. Man erkennt aus den Gleichungen (1), dass vom Zeiger 0 an jeder spätere Zähler oder Nenner eines Näherungsbruches grösser ist, als der vorhergehende.

VII. Aus denselben Gleichungen ergibt sich auch sofort folgende Formel zur Bestimmung der Quotienten durch die Zähler oder Nenner der Näherungsbrüche

3) $$a_n = \frac{M_n - M_{n-2}}{M_{n-1}} = \frac{N_n - N_{n-2}}{N_{n-1}}$$

§. 4. Beziehung zwischen den Zählern und Nennern zweier benachbarter Näherungsbrüche.

Aus den im vorstehenden Paragraphen entwickelten allgemeinen Beziehungen und den Werthen $M_{-2} = 0$, $N_{-2} = 1$, $M_{-1} = 1$, $N_{-1} = 0$, $M_0 = a_0$, $N_0 = 1$ folgt

$$M_{-1}N_{-2} - M_{-2}N_{-1} = 1.1 - 0.0 = 1 = (-1)^{-2}$$
$$M_0 N_{-1} - M_{-1} N_0 = a_0.0 - 1.1 = -1 = (-1)^{-1}$$
$$M_1 N_0 - M_0 N_1 = (a_1 M_0 + M_{-1}) N_0 - M_0 (a_1 N_0 + N_{-1})$$
$$= -(M_0 N_{-1} - M_{-1} N_0) = -(-1) = 1 = (-1)^0$$
$$M_2 N_1 - M_1 N_2 = (a_2 M_1 + M_0) N_1 - M_1 (a_2 N_1 + N_0)$$
$$= -(M_1 N_0 - M_0 N_1) = -1 = (-1)^1$$

Hieraus abstrahiren wir das allgemeine Gesetz

1) $$M_n N_{n-1} - M_{n-1} N_n = (-1)^{n-1}$$

Denn angenommen, diese Beziehung sei richtig für einen gewissen Werth von n; so hat man

$$M_{n+1} N_n - M_n N_{n+1} = (a_{n+1} M_n + M_{n-1}) N_n - M_n (a_{n+1} N_n + N_{n-1})$$
$$= -(M_n N_{n-1} - M_{n-1} N_n) = -(-1)^{n-1} = (-1)^n.$$

Das fragliche Gesetz gilt also alsdann auch für $n+1$. Nun ist seine Richtigkeit bereits für $n = -1, 0, 1, 2$ nachgewiesen; dasselbe ist also allgemein gültig.

Statt $M_n N_{n-1} - M_{n-1} N_n = (-1)^{n-1}$ kann man auch schreiben

2) $$M_{n-1} N_n - M_n N_{n-1} = (-1)^n$$ und auch

3) $$M_n N_{n+1} - M_{n+1} N_n = (-1)^{n+1}$$

Der absolute Werth der Grössen auf der linken Seite dieser Gleichungen ist also stets $= 1$. Derselbe wechselt regelmässig das Zeichen, wenn der Index n um Eine Einheit wächst. Der Exponent von -1 auf der rechten Seite ist stets gleich dem Zeiger des Nenners N in dem additiven Gliede auf der linken Seite.

§. 5. *Zähler und Nenner eines Näherungsbruches sind relative Primzahlen.*

Denn da $M_n N_{n-1} - M_{n-1} N_n = \pm 1$ ist; so können zwei Zahlen wie M_n und N_n, welche Zähler und Nenner Ein und desselben Näherungsbruches K_n sind, ausser 1 kein gemeinschaftliches Maass besitzen, indem ja sonst die linke Seite dieser Gleichung, folglich auch die rechte Seite ± 1 durch jenes Maass theilbar sein müsste, was unmöglich ist.

Demnach ergeben sich alle Näherungsbrüche und auch der letzte K_r, welcher den Gesammtwerth des Kettenbruchs K darstellt, durch das Verfahren in §. 3 stets in der kürzesten Form.

§. 6. *Werthverhältniss zwischen den Näherungsbrüchen.*

I. Durch Division der Gleichung $M_{n+1} N_n - M_n N_{n+1} = (-1)^n$ mit $N_n N_{n+1}$ ergibt sich

$$1)\quad \frac{M_{n+1}}{N_{n+1}} - \frac{M_n}{N_n} = K_{n+1} - K_n = \frac{(-1)^n}{N_n N_{n+1}}$$

Da die Werthe von N_n und N_{n+1} mit dem Zeiger n wachsen; so folgt, dass der absolute Werth der Differenz zwischen zwei benachbarten Näherungsbrüchen K_{n+1} und K_n immer kleiner wird, je mehr n zunimmt, und zwar ist der absolute Betrag dieser Differenz stets ein Bruch, dessen Zähler 1 und dessen Nenner das Produkt $N_n N_{n+1}$ aus den Nennern jener beiden Näherungsbrüche ist.

Das Zeichen dieser Differenz wechselt regelmässig zwischen $+$ und $-$, und es ist klar, dass ein Näherungsbruch K_{n+1} grösser oder kleiner, als der vorhergehende K_n ist, je nachdem sein Zeiger $_{n+1}$ unpaar oder paar ist.

Demnach hat man $K_1 > K_0$, $K_3 > K_2$, $K_5 > K_4$, ... Auch für die Zeiger -1 und -2 gilt diese Beziehung $K_{-1} > K_{-2}$, indem man $K_{-1} = \frac{1}{0} = \infty$, $K_{-2} = \frac{0}{1} = 0$ hat.

II. Um jetzt einen Näherungsbruch K_n mit dem Gesammtwerthe K des Kettenbruchs zu vergleichen, haben wir nach §. 3 und 4

$$K - K_n = \frac{M_n + M_{n-1} x_n}{N_n + N_{n-1} x_n} - \frac{M_n}{N_n} = \frac{(M_{n-1} N_n - M_n N_{n-1}) x_n}{N_n (N_n + N_{n-1} x_n)} \quad \text{oder}$$

$$2)\quad K - K_n = \frac{(-1)^n x_n}{N_n (N_n + N_{n-1} x_n)}$$

und auch, wenn man $x_n = \frac{1}{a_{n+1} + x_{n+1}}$ setzt,

$$3)\quad K - K_n = \frac{(-1)^n}{N_n (N_{n+1} + N_n x_{n+1})}$$

Erhöhet man in der Gleichung (2) alle Zeiger um 1, so kommt

$$4)\qquad K - K_{n+1} = \frac{(-1)^{n+1} x_{n+1}}{N_{n+1}(N_{n+1} + N_n x_{n+1})}$$

Diese Differenz $K - K_{n+1}$, verglichen mit der Differenz $K - K_n$ aus Gl. (3), ergibt

$$5)\qquad K - K_{n+1} = -(K - K_n) \cdot \frac{N_n x_{n+1}}{N_{n+1}}$$

Da $N_{n+1} > N_n$ und $x_{n+1} < 1$, also noch weit mehr $\frac{N_n x_{n+1}}{N_{n+1}} < 1$ ist; so folgt, dass die Differenz $K - K_{n+1}$ nach ihrem absoluten Werthe kleiner ist, als die Differenz $K - K_n$, dass sie aber das entgegengesetzte Zeichen besitzt. Von dem ersteren Theile dieses Satzes macht nur der Fall für den Zeiger $n = -2$ eine Ausnahme, indem hierfür $N_{n+1} = N_{-1} = 0$ und die Differenz $K - K_{-1} = -\infty$ ist, während die vorhergehende $K - K_{-2} = K$ ist.

Hiernach sind also die Näherungsbrüche von den sukzessiv höheren Zeigern abwechselnd grösser und kleiner, als der Werth K des Kettenbruchs, indem alle Näherungsbrüche von unpaaren Zeigern grösser, von paaren Zeigern dagegen kleiner sind; sie nähern sich übrigens dem Werthe K immer mehr und mehr, und hierin liegt der Grund ihrer Benennung.

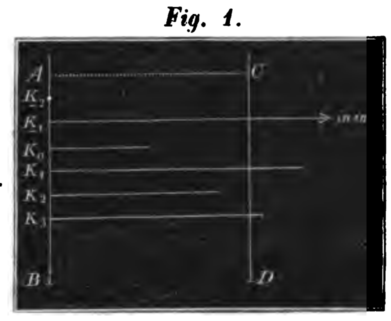
III. Was die Fehlergränze oder den höchsten Betrag des Fehlers betrifft, welchen man begehen kann, wenn man den Näherungsbruch K_n für den Werth K des ganzen Kettenbruchs nimmt; so ist nach Vorstehendem der absolute Betrag der Differenz $K - K_n$

$$\frac{1}{N_n(N_{n+1} + N_n x_{n+1})} < \frac{1}{N_n N_{n+1}} < \frac{1}{N_n N_n} \text{ oder } < \frac{1}{N_n^2}$$

Der fragliche Fehler kann also niemals den Werth des Bruches $\frac{1}{N_n N_{n+1}}$, noch viel weniger aber den Werth von $\frac{1}{N_n^2}$, also den Werth eines Bruches, dessen Zähler 1 und dessen Nenner das Quadrat des Nenners des fraglichen Näherungsbruches ist, übersteigen.

IV. Alle diese Eigenschaften kann man leicht an den Näherungswerthen des in §. 3 beispielsweise entwickelten Kettenbruchs $[3, 2, 5, 1, 4, 7] = \frac{1571}{454}$ bestätigen, worin man $K_{-2} = \frac{0}{1}$, $K_{-1} = \frac{1}{0}$, $K_0 = \frac{3}{1}$, $K_1 = \frac{7}{2}$, $K_2 = \frac{38}{11}$, $K_3 = \frac{45}{13}$, $K_4 = \frac{213}{63}$ hat.

Fig. 1.



In Fig. 1 sind diese Beziehungen graphisch dargestellt. Der Werth K ist der Abstand der beiden Parallelen AB, CD. K_{-2}, K_{-1}, K_0, K_1, $K_2 \ldots$ sind die Längen der auf AB in den gleichnamigen Punkten errichteten Perpendikel, deren Endpunkte abwechselnd auf die linke und auf die rechte Seite von CD fallen, der letztern Linie aber vom Zeiger $n = -1$ an immer näher kommen.

V. In der oben gefundenen Beziehung (3)

$$K = K_n + \frac{(-1)^n}{N_n(N_{n+1} + N_n x_{n+1})} = K_n + \frac{(-1)^n}{N_n\left[N_{n-1} + N_n(a_{n+1} + x_{n+1})\right]}$$

hängen die Grössen mit den Zeigern $n-1$ und n von den ersten Quotienten $a_0, a_1, \ldots a_n$, dagegen die Grösse $a_{n+1} + x_{n+1}$ von den darauf folgenden Quotienten $a_{n+1}, a_{n+2} \ldots a_r$ allein ab, und es ist offenbar $a_{n+1} + x_{n+1} = [a_{n+1}, a_{n+2}, \ldots a_r]$ der Werth des Kettenbruchs, welcher die Ganzen a_{n+1} enthält, während $x_{n+1} = [0, a_{n+2}, \ldots a_r]$ der Werth jenes Kettenbruchs ohne die Ganzen a_{n+1} ist. Wie man also auch die auf a_{n+1} folgenden Quotienten nach Grösse und Anzahl verändern möge, x_{n+1} bleibt stets ein echter Bruch, und es ist klar, dass die Veränderung des Quotienten a_{n+1} um eine einzige Einheit auf den Gesammtwerth K des Kettenbruchs einen grösseren Einfluss hat, als jede mögliche Veränderung der darauf folgenden Quotienten.

§. 7. ***Zwischen zwei benachbarte Näherungsbrüche K_n und K_{n+1} kann kein Bruch eingeschaltet werden, welcher sich mit kleineren Zahlen schreiben liesse, als der aus den grössten Zahlen bestehende letztere Näherungsbruch K_{n+1}.***

I. Denn man hat

$$K_n = \frac{M_n}{N_n} = \frac{M_n N_{n+1}}{N_n N_{n+1}} \quad \text{und} \quad K_{n+1} = \frac{M_{n+1}}{N_{n+1}} = \frac{M_{n+1} N_n}{N_n N_{n+1}}$$

Hierin hat immer K_{n+1} die grösseren Zahlen im Zähler und Nenner, ob aber K_n oder K_{n+1} der grössere Bruch sei, hängt davon ab, ob n unpaar oder paar ist. Wäre K_n der kleinere Bruch, so hätte man $M_{n+1} N_n - M_n N_{n+1} = 1$, also $M_{n+1} N_n = M_n N_{n+1} + 1$. Ein jeder zwischen K_n und K_{n+1} liegende

Werth kann demnach, wenn $\frac{p}{q}$ irgend einen echten Bruch auf seiner kleinsten Benennung darstellt, sodass $q > p$ und q mit p relativ prim ist, ausgedrückt werden durch

$$\frac{M_n N_{n+1} + \frac{p}{q}}{N_n N_{n+1}} = \frac{q M_n N_{n+1} + p}{q N_n N_{n+1}}$$

Sollte es nun möglich sein, dass sich der letztere Bruch mit kleineren Zahlen schreiben liesse, als K_{n+1}; so müsste sich der Zähler $q M_n N_{n+1} + p$ so weit gegen den Nenner $q N_n N_{n+1}$ aufheben lassen, dass im Zähler eine Zahl $< M_{n+1}$ und im Nenner eine Zahl $< N_{n+1}$ zurückbliebe.

Da aber ein jeder Faktor von q im ersten Theil $q M_n N_{n+1}$, nicht aber im zweiten Theile p des fraglichen Zählers enthalten ist; so wird sich jener Bruch nicht durch einen Faktor von q aufheben lassen. Es wird also q im Nenner $q N_n N_{n+1}$ stehen bleiben.

Da ein jeder Faktor von N_{n+1} im ersten Theile $q N_n N_{n+1}$ des Zählers enthalten ist; so muss, wenn der Bruch durch einen solchen Faktor a aufhebbar sein sollte, auch der zweite Theil p durch a theilbar sein. Angenommen, Dies sei der Fall und a das grösste gemeinschaftliche Maass zwischen N_{n+1} und p; so erhielte man durch Aufhebung mit a

$$\frac{q M_n \left(\frac{N_{n+1}}{a}\right) + \left(\frac{p}{a}\right)}{q N_n \left(\frac{N_{n+1}}{a}\right)}$$

Ob sich nun dieser Bruch ferner noch durch einen Faktor von N_n aufheben lässt, oder nicht, ist gleichgültig. Es wird im Nenner stets das Produkt $q \frac{N_{n+1}}{a}$, worin a höchstens $= N_{n+1}$ sein kann, stehen bleiben. Da aber $q > p$, also $\frac{q}{a} > \frac{p}{a}$ ist; so muss, weil $\frac{p}{a}$ eine ganze Zahl, also $\geqq 1$ ist, $\frac{q}{a} > 1$, folglich $q \frac{N_{n+1}}{a} > N_{n+1}$ sein. Der Nenner des fraglichen Bruches wird also jedenfalls grösser als der Nenner des mit den grössten Zahlen geschriebenen Näherungsbruches K_{n+1} sein.

Was den Zähler anlangt; so muss derselbe, selbst wenn sich der Bruch noch durch den ganzen Werth von N_n heben liesse, mindestens gleich $\frac{q M_n \left(\frac{N_{n+1}}{a}\right) + \left(\frac{p}{a}\right)}{N_n}$ bleiben.

Da aber $q > p$; so ist dieser Ausdruck offenbar $> (M_n N_{n+1} + 1) \frac{p}{a N_n}$ oder weil $M_n N_{n+1} + 1 = M_{n+1} N_n$ ist, $> \frac{p M_{n+1}}{a}$, mithin auch, weil a nicht grösser sein kann als p, $> M_{n+1}$. Es wird also auch der Zähler des fraglichen Bruches grösser sein, als der Zähler von K_{n+1}.

II. Aus Vorstehendem folgt, dass jeder zwischen K_n und K_{n+1} liegende Bruch nicht allein einen grösseren Zähler, sondern auch einen grösseren Nenner hat, als K_{n+1}.

Von den beiden Näherungsbrüchen K_n und K_{n+1} kommt K_{n+1} dem Werthe K am nächsten, besitzt aber die grösseren Zahlen. Ein jeder Bruch nun, dessen Zähler oder dessen Nenner kleiner ist, als resp. der Zähler oder Nenner von K_{n+1}, entfernt sich nach Obigem weiter von K als der Näherungsbruch K_{n+1}, und wenn jener neue Bruch auf der entgegengesetzten Seite von K, also auf derselben Seite wie K_n liegt; so entfernt er sich sogar weiter von K, als K_n, wenn er nicht gleich K_n selbst ist.

§. 8. Mittelbrüche.

I. Zwischen zwei unmittelbar aufeinander folgende Näherungsbrüche K_n und K_{n+1} lassen sich keine Brüche mit kleineren Zahlen einschalten.

Wol aber lassen sich zuweilen zwischen einen Näherungsbruch K_n und den zuzweit darauf folgenden K_{n+2} Brüche einschalten, welche zwar grössere Zahlen, als K_n und K_{n+1}, aber kleinere, als K_{n+2} haben. Diese zwischen K_n und K_{n+2} liegenden Werthe, welche entweder sämmtlich $< K$ oder sämmtlich $> K$ sind, jenachdem K_n und K_{n+2} beide $< K$ oder beide $> K$ sind, entfernen sich von dem Werthe K zwar weiter, als K_{n+2}; jedoch liegen dieselben hinundwieder, wenigstens zum Theil, näher an K, als K_{n+1}, obgleich auf entgegengesetzter Seite wie K_{n+1}. Man nennt diese Werthe, deren Anzahl stets eine begränzte ist, Mittelbrüche. Dieselben lassen sich folgendermaassen darstellen.

Wenn n paar, also K_n und $K_{n+2} < K$, dagegen $K_{n+1} > K$; so ist die Reihenfolge der Näherungswerthe K_n, K_{n+1}, K_{n+2} der Grösse nach, sodass die grösseren auf die kleineren folgen, diese

$$K_n \quad < \quad K_{n+2} \quad < \quad K_{n+1}$$

$$\text{oder } \frac{M_n}{N_n} \qquad \frac{M_{n+2}}{N_{n+2}} \qquad \frac{M_{n+1}}{N_{n+1}}$$

$$\text{oder } \frac{M_n}{N_n} \qquad \frac{a_{n+2} M_{n+1} + M_n}{a_{n+2} N_{n+1} + N_n} \qquad \frac{M_{n+1}}{N_{n+1}}$$

Ist der Quotient $a_{n+2} > 1$; so gibt es zwischen K_n und K_{n+2} Mittelbrüche, und zwar deren $a_{n+2} - 1$. Dieselben haben folgende Werthe, welche der Grösse nach geordnet sind,

$$\frac{M_{n+1}+M_n}{N_{n+1}+N_n}, \quad \frac{2M_{n+1}+M_n}{2N_{n+1}+N_n}, \quad \frac{3M_{n+1}+M_n}{3N_{n+1}+N_n}, \quad \ldots \frac{(a_{n+2}-1)\,M_{n+1}+M_n}{(a_{n+2}-1)\,N_{n+1}+N_n}$$

Dass die Zähler und Nenner dieser Mittelbrüche grösser sind, als die Zähler und Nenner der beiden Näherungsbrüche K_n und K_{n+1}, dagegen kleiner, als die Zähler und Nenner des Näherungsbruches K_{n+2}, leuchtet ein.

Wenn n unpaar, also K_n und $K_{n+2} > K$, dagegen $K_{n+1} < K$; so erhält man genau dieselben Formeln und Resultate, mit der Modifikation, dass die vorstehenden Reihenfolgen nicht vom Kleinern zum Grössern, sondern vom Grössern zum Kleinern fortschreiten.

II. Bezeichnet man einen zwischen K_n und K_{n+2} liegenden Mittelbruch wie $\frac{pM_{n+1}+M_n}{pN_{n+1}+N_n}$ mit $K_p^{(n)} = \frac{M_p^{(n)}}{N_p^{(n)}}$; so hat man für die Zähler und Nenner zweier benachbarter Mittelbrüche in dem Zwischenraum von K_n auf K_{n+2} die Beziehung

$$M_{p+1}^{(n)}N_p^{(n)} - M_p^{(n)}N_{p+1}^{(n)} = [(p+1)M_{n+1}+M_n]\,[pN_{n+1}+N_n] - [pM_{n+1}+M_n]\,[(p+1)N_{n+1}+N_n] = M_{n+1}N_n - M_nN_{n+1} = (-1)^n$$

Hieraus folgt sofort wie in §. 5 und 7, dass Zähler und Nenner eines Mittelbruchs relative Primzahlen sind, auch dass sich zwischen zwei benachbarte Mittelbrüche keine anderen Brüche einschalten lassen, welche sich mit kleineren Zahlen schreiben liessen, als der aus den grössten Zahlen bestehende Mittelbruch.

III. Was die Differenz zwischen zwei unmittelbar aufeinander folgenden Mittelbrüchen betrifft; so hat man, wenn man die vorstehende Formel durch $N_p^{(n)}\,N_{p+1}^{(n)}$ dividirt,

$$K_{p+1}^{(n)} - K_p^{(n)} = \frac{M_{p+1}^{(n)}}{N_{p+1}^{(n)}} - \frac{M_p^{(n)}}{N_p^{(n)}} = \frac{(-1)^n}{N_p^{(n)}\,N_{p+1}^{(n)}}$$

Diese Differenz ist also gleich einem Bruche, dessen Zähler $(-1)^n$, und dessen Nenner das Produkt der Nenner der beiden Mittelbrüche ist.

IV. Die Differenz zwischen dem Werthe K des ganzen Kettenbruchs und dem $p$ten Mittelbruche $K_p^{(n)}$ ist

$$K - K_p^{(n)} = \frac{M_{n+1} + M_n x_{n+1}}{N_{n+1} + N_n x_{n+1}} - \frac{p M_{n+1} + M_n}{p N_{n+1} + N_n}$$

$$= \frac{(-1)^n (1 - p x_{n+1})}{(p N_{n+1} + N_n)(N_{n+1} + N_n x_{n+1})}$$

oder da $x_{n+1} = \frac{1}{a_{n+2} + x_{n+2}}$ ist,

$$K - K_p^{(n)} = \frac{(-1)^n (a_{n+2} - p + x_{n+2})}{(pN_{n+1} + N_n)\left[pN_{n+1} + N_n + N_{n+1}(a_{n+2} - p + x_{n+2})\right]}$$

Der absolute Werth dieser Differenz ist offenbar stets

$$< \frac{a_{n+2} + 1 - p}{(p N_{n+1} + N_n)(p N_{n+1} + N_n)} \text{ oder } < \frac{a_{n+2} + 1 - p}{(p N_{n+1} + N_n)^2}$$

Der Fehler, wenn man $K_p^{(n)}$ statt K setzt, ist also kleiner, als ein Bruch, dessen Zähler $a_{n+2} + 1 - p$ und dessen Nenner das Quadrat des Nenners des Mittelbruchs ist.

§. 9. *Darstellung der Mittelbrüche als Werthe vollständiger Kettenbrüche.*

I. Denkt man sich in dem Werthe eines zwischen K_n und K_{n+2} liegenden Mittelbruchs

$$K_p^{(n)} = \frac{p M_{n+1} + M_n}{p N_{n+1} + N_n}$$

unter p den Quotienten eines Kettenbruchs, welcher an der Stelle von a_{n+2} steht; so stellt dieser Mittelbruch den Werth des Kettenbruchs $[a_0, a_1, a_2 \ldots a_{n+1}, p]$ dar.

So sind z. B. in dem Kettenbruche $[3, 7, 15, 1, 25]$ die zwischen den Näherungswerthen $K_0 = 3$ und $K_2 = [3, 7, 15] = \frac{333}{106}$ liegenden $15 - 1 = 14$ Mittelbrüche, da $K_1 = [3, 7] = \frac{22}{7}$ ist, diese

$$\frac{1.22 + 3}{1.7 + 3} = \frac{25}{8}, \frac{2.22 + 3}{2.7 + 3} = \frac{47}{15}, \frac{3.22 + 3}{3.7 + 3} = \frac{69}{22} \ldots$$

$$\ldots \frac{13.22 + 3}{13.7 + 1} = \frac{289}{92}, \frac{14.13 + 3}{14.7 + 1} = \frac{311}{99}$$

und dieselben sind resp. gleich den Werthen der Kettenbrüche $[3, 7, 1]$, $[3, 7, 2]$, $[3, 7, 3]$ . . $[3, 7, 13]$, $[3, 7, 14]$.

II. Hiernach kann man die Mittelbrüche zwischen K_n und K_{n+2} auch während der Berechnung von K nach dem Schema §. 3 einschalten, nachdem man K_{n+1} gebildet hat, und zwar nach folgendem Schema für die zwischen K_0 und K_2 des Kettenbruchs $[3, 7, 15, 1, 25]$ liegenden Mittelbrüche

n	a_n	p	M_n	N_n	$M_p^{(0)}$.	$N_p^{(0)}$.
—2			0	1		
—1			1	0		
0	3		3	1		
1	7		22	7		
		1			25	8
		2			47	15
		3			69	22
		.			.	.
		.			.	.
		.			.	.
		14			311	99
2	15		333	106		
3	1		355	113		
4	25		9208	2931		

III. Es wird auch noch darauf aufmerksam gemacht, dass von zwei benachbarten Mittelbrüchen $[a_0, a_1 \ldots a_{n+1}, p]$ und $[a_0, a_1 \ldots a_{1+1}, (p+1)]$ der spätere, wenn man $p+1 = p+\frac{1}{1}$ schreibt, in die Form $[a_0, a_1 \ldots a_{n+1}, p, 1]$ gebracht werden kann, wonach beide Mittelbrüche als zwei benachbarte Näherungsbrüche Ein und desselben Kettenbruchs erscheinen, dessen erste Quotienten $a_0, a_1 \ldots a_{n+1}, p, 1$ sind.

IV. Allgemein aber können alle Näherungsbrüche wie Mittelbrüche angesehen werden, indem jede Reihe von Mittelbrüchen mit Einem Näherungsbruche K_n beginnt und mit einem anderen K_{n+2} schliesst. Diese Anschauung ist auch dann richtig, wenn der Quotient $a_{n+2} = 1$ ist, indem alsdann K_n und K_{n+2} die einzigen Glieder der betreffenden Reihe sind.

§. 10. *Entwickelung eines gemeinen Bruches in einen Kettenbruch mit grössten Subquotienten.*

I. Wenn a_0 die grössten in dem Bruche $\frac{M}{N}$ enthaltenen Ganzen oder der bei der gewöhnlichen Division mit N in M sich ergebende Quotient und R_0 der hierbei verbleibende Rest ist; so hat man die Gleichung

1) $\frac{M}{N} = a_0 + \frac{R_0}{N}$ oder

2) $M = a_0 N + R_0$

In der Gleichung (1) heisse der Werth $\frac{R_0}{N}$ der Restbruch zur Unterscheidung von dem Reste R_0.

Durch den Quotienten a_0 ist der Werth des Bruches $\frac{M}{N}$ nicht vollständig erschöpft; es muss vielmehr noch ein Restbruch $\frac{R_0}{N}$ hinzuaddirt werden, welcher entschieden positiv ist, so-dass der Rest R_0 mit dem Divisor N gleiches Zeichen hat. Der Restbruch ist auch < 1 und kann bis auf 0 herabsinken, der Rest R_0 ist demnach $< N$ und kann ebenfalls auf 0 herabsinken.

Nähme man für den Quotienten eine ganze Zahl $< a_0$ an; so würde zwar der Restbruch ebenfalls positiv bleiben, aber $\geqq 1$, also der Rest $\geqq N$ werden. In beiden Fällen, wo also der Restbruch positiv ist, nennen wir den Quotienten einen Subquotienten, im ersteren Falle den grössten Subquotienten.

Nähme man für den Quotienten die ganze Zahl $a_0 + 1$ an; so würde der Restbruch negativ werden, indess nach seinem absoluten Werthe $\leqq 1$ sein; der Rest würde also das entgegengesetzte Zeichen des Divisors N annehmen, jedoch numerisch nicht grösser, als derselbe werden. Nähme man aber den Quotienten noch grösser; so würde in dem negativen Restbruche der numerische Werth des Restes den des Divisors übersteigen. In beiden Fällen, wo also der Restbruch negativ ist, heisse der Quotient ein Superquotient, und im ersteren Falle der kleinste Superquotient.

II. Vorläufig werden wir uns nur mit grössten Subquotienten zu thun machen, wie sie bei der gewöhnlichen Division der Zahlen entstehen. Wir betrachten sofort nebeneinander zwei Brüche $\frac{M}{N}$ und $\frac{Mp}{Np}$, wovon Zähler und Nenner im ersten relativ prim sind, im zweiten jedoch das grösste gemeinschaftliche Maass p haben. Die Brüche können echt oder unecht sein: wären sie echt; so hätte man stets für den ersten Quotienten den Werth 0, was der Allgemeinheit der nachfolgenden Rechnung keinen Eintrag thut. Dividirt man nach der für die Aufsuchung des grössten gemeinschaftlichen Maasses zwischen zwei Zahlen bekannten Methode erst mit dem Nenner in den Zähler, dann mit dem verbleibenden Reste in den vorhergehenden Divisor u. s. f., indem man die Quotienten sukzessive mit $a_0, a_1, a_2 \ldots a_r$ und die Reste von $\frac{M}{N}$ mit $R_0, R_1, R_2 \ldots R_r$, diejenigen von $\frac{Mp}{Np}$ dagegen mit $R_0p, R_1p, R_2p \ldots R_rp$,

bezeichnet; so ergibt sich

$$\begin{array}{llll}
M = a_0 N + R_0 & R_0 < N & Mp = a_0 Np + R_0 p & R_0 p < Np \\
N = a_1 R_0 + R_1 & R_1 < R_0 & N_0 p = a_1 R_0 p + R_1 p & R_1 p < R_0 p \\
R_0 = a_2 R_1 + R_2 & R_2 < R_1 & R_0 p = a_2 R_1 p + R_2 p & R_2 p < R_1 p \\
R_1 = a_3 R_2 + R_3 & R_3 < R_2 & R_1 p = a_3 R_2 p + R_3 p & R_3 p < R_2 p \\
\cdot & \cdot & \cdot & \\
\cdot & & \cdot & \\
\cdot & & \cdot & \\
\cdot & & \cdot & \\
R_{r-4} = a_{r-2} R_{r-3} + R_{r-2} & R_{r-2} < R_{r-3} & R_{r-4} p = a_{r-2} R_{r-3} p + R_{r-2} p & R_{r-2} p < R_{r-3} p \\
R_{r-3} = a_{r-1} R_{r-2} + 1 & 1 < R_{r-2} & R_{r-3} p = a_{r-1} R_{r-2} p + p & p < R_{r-2} p \\
R_{r-2} = R_{r-2} \,.\, 1 + 0 & 0 < 1 & R_{r-2} p = R_{r-2} \,.\, 1p + 0 & 0 < p \\
\quad = a_r \,.\, 1 + 0 & & \quad = a_r \,.\, 1p + 0 &
\end{array}$$

In beiden Fällen hat man

$$\frac{M}{N} \text{ oder } \frac{Mp}{Np} = \frac{a_0 N + R_0}{N} = a_0 + \frac{R_0}{N}$$

$$= a_0 + \frac{1}{\frac{N}{R_0}} = a_0 + \frac{1}{\frac{a_1 R_0 + R_1}{R_0}} = a_0 + \frac{1}{a_1 + \frac{R_1}{R_0}}$$

u. s. w.; überhaupt

$$\frac{M}{N} = \frac{Mp}{Np} = [a_0, a_1, a_2, \ldots a_r]$$

III. Hierdurch ist der gegebene Bruch in einen Kettenbruch entwickelt. Man sieht, dass das gemeinschaftliche Maass p, welches der Zähler und Nenner des gegebenen Bruches etwa besitzt, bei dieser Entwickelung verschwindet, ein Resultat, welches mit §. 5 übereinstimmt, wonach der reduzirte Kettenbruch immer den ihm gleichen gemeinen Bruch a u f k l e i n s t e r B e n e n n u n g erzeugt.

Ausserdem erkennt man — unter der Voraussetzung des Prinzips der g r ö s s t e n S u b q u o t i e n t e n — dass der einem rationalen Bruche gleiche Kettenbruch stets eine e n d l i c h e L ä n g e besitzt, dass sich jeder Bruch nur a u f e i n e e i n z i g e W e i s e als Kettenbruch darstellen lässt, dass k e i n e z w e i von einander irgendwie a b w e i c h e n d e Kettenbrüche Ein und denselben Zahlenwerth haben können, und dass der Quotient 0 nur bei echten Brüchen a n d e r o b e r s t e n S t e l l e als a_0 vorkommen kann.

So hat man z. B. für $\frac{1571}{454} = [3, 2, 5, 1, 4, 7]$

454 | 1571 | 3 . . . . a_0
    1362
     209 | 454 | 2 . . . . a_1
           418
            36 | 209 | 5 . . . . a_2
                 180
                  29 | 36 | 1 . . . . a_3
                       29
                        7 | 29 | 4 . . . . a_4
                            28
                             1 | 7 | 7 . . . . a_5
                                 7
                                 0

und für $\frac{11}{263} = [0, 23, 1, 10]$

263 | 11 | 0 . . . . a_0
       0
      11 | 263 | 23 . . . . a_1
           22
           43
           33
           10 | 11 | 1 . . . . a_2
                10
                 1 | 10 | 10 . . . . a_3
                     10
                      0

IV. Es wird schliesslich noch bemerkt, dass der letzte Quotient a_n bei einer solchen Entwickelung niemals $= 1$ werden kann, weil in dem Schlusse $a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{1}}$ nicht a_{n-1}, sondern $a_{n-1} + \frac{1}{1} = a_{n-1} + 1$ der grösste Subquotient sein und demnach jener Schluss die Form $a_{n-2} + \frac{1}{a_{n-1} + 1}$ annehmen würde.

§. 11. *Fall, wo der Zähler oder Nenner des zu entwickelnden Bruches unvollständig gegeben ist.*

I. Wenn der als Kettenbruch darzustellende Bruch nicht genau, sondern nur in den höchsten Stellen der ihm gleichen dekadischen Zahl gegeben ist, wie z. B. wenn der Werth der

bekannten Zahl π als $3,14159\ldots = \frac{314159\cdots}{100000000}$ gegeben wäre; so kann man zwar mit Bestimmtheit behaupten, dass unter Weglassung der unbestimmten Stellen die genaue Zahl 3, 14159 höchstens um Eine Einheit der letzten Dezimalstelle, also höchstens um $\frac{1}{100000}$ falsch sein kann; allein ganz anders verhält es sich mit dem Kettenbruche, welcher durch die Entwickelung der genauen Zahl $3,14159 = \frac{314159}{100000}$ entstehen würde. Derselbe ist [3, 7, 15, 1, 25, 1, 7, 4]; man würde sich aber sehr täuschen, wenn man glauben wollte, in diesem Kettenbruche läge der Fehler gegen den wahren Werth von π erst im letzten Quotienten 4. Dass Dies bei weitem nicht der Fall ist, erkennt man sofort, wenn man den genaueren Werth 3, 1415927 in den Kettenbruch [3, 7, 15, 1, 354, 2, 6, 1, 4, 1, 2] entwickelt. Dieser stimmt nur bis zum vierten Quotienten mit dem früheren überein, und schon der fünfte Quotient weicht nicht um wenige, sondern um 326 Einheiten von dem früheren ab. Da nun Eine Einheit in einem höheren Quotienten mehr gilt, als alle folgenden zusammengenommen; so leuchtet ein, dass die Darstellung der letzten Quotienten 25, 1, 7, 4 in der ersten Entwickelung eine ganz fruchtlose, ja in mancher Beziehung schädliche Arbeit ist, da sie leicht zu Irrungen über die Fehlergränze Veranlassung geben kann.

Hiernach ist es von Wichtigkeit, wenn Zähler oder Nenner des gegebenen Bruches oder Beide unvollständig sind, den letzten genau darstellbaren Quotienten des Kettenbruchs, welcher also höchstens um eine einzige Einheit von der Wahrheit abweichen kann, zu erkennen, und bei diesem die Kettenbruchsentwickelung abzubrechen.

Hierzu gelangt man, wenn man die zu dieser Entwickelung nöthigen Divisionen nach den für das Rechnen mit verkürzten Zahlen bestehenden Regeln ausführt, die Quotienten nur bis zur Ordnung der Einer entwickelt, bei den verbleibenden Resten aber, welche selbst verkürzte Zahlen sind, den grösstmöglichen Fehler der letzten Ziffern ermittelt und hiernach diese letzten Ziffern entweder ganz und gar wie unbestimmte bezeichnet, oder doch auf den darin möglicherweise enthaltenen Fehler bei der späteren Rechnung Rücksicht nimmt.

Entwickelt man hiernach die Zahl $\pi = 3,1415926\ldots$ in einen Kettenbruch und bezeichnet ganz unbestimmte Ziffern mit Sternen, solche jedoch, welche höchstens um Eine bis zwei Einheiten zu gross oder zu klein sein können, durch einen resp.

darüber oder darunter gesetzten Punkt, markirt auch den Rang der Zahlen durch Einschaltung eines Dezimalkommas; so ergibt sich folgende Rechnung

```
10000000,|31415926,|...| 3
          30000000 |
          ---------
           1415926,|...| 10000000,|000| 7
                          991148. |
                         ---------
                          8852.., | .. | 14159 |26,..| 15
                                          8852 |
                                          ----
                                          5307 |
                                          4426 |
                                          ----
                                           881.|..,..| 885 |2.,..| 1
                                                        881 |
                                                        ---
                                                          4.|..,..
```

Die Operation ist offenbar bei dem Quotienten $a_3 = 1$ abzubrechen; spätere Quotienten lassen sich durchaus nicht mit einer erkennbaren Genauigkeit angeben, und man kann behaupten, dass der wahre Werth von $\pi = [3, 7, 15, 1 \ldots]$ ist, worin der letzte Quotient 1 nicht um eine volle Einheit zu klein sein, auch dass der Werth des Kettenbruchs [3, 7, 15, 1] um nicht mehr als $\frac{1}{10000000}$ von dem wahren Werthe π differiren kann.

II. Man kann übrigens auch folgendermaassen verfahren. Der kleinstmögliche Werth einer unvollständigen Dezimalzahl wie 3,1415926... wird erhalten, wenn man in die unbestimmten Stellen lauter Nullen setzt, oder dieselben weglässt; Dies gibt hier 3,1415926. Der grösstmögliche Werth dagegen ergibt sich, wenn man in jene Stellen lauter Neunen setzt, oder bei Weglassung derselben die letzte bestimmte Ziffer um Eine Einheit erhöhet; Dies gibt hier 3,1415927. Zwischen diesen beiden Gränzen liegt der Werth von π. Entwickelt man beide Gränzwerthe in Kettenbrüche; so zeigt sich durch die Übereinstimmung der Quotienten vom Anfange herab, wie weit die Quotienten unbedingt beizubehalten sind. Da man findet

$$3,1415926 = [3, 7, 15, 1, 243, 1, 1, 10, 1, 1, 4]$$
$$3,1415927 = [3, 7, 15, 1, 354, 2, 6, 1, 4, 1, 2]$$ so ist
$$\pi = 3,1415926 \ldots = [3, 7, 15, 1, \ldots]$$

Reduzirt man den Kettenbruch [3, 7, 15, 1] wiederum auf einen gemeinen; so erhält man unter den Näherungsbrüchen mehrere der in der Praxis vorkommenden abgekürzten Werthe von π, nämlich

n	a_n	M_n	N_n	K_n
-2		0	1	
-1		1	0	
0	3	3	1	$\frac{3}{1}$
1	7	22	7	$\frac{22}{7}$
2	15	333	106	$\frac{333}{106}$
3	1	355	113	$\frac{355}{113}$

§. 12. Independentes Bildungsgesetz der Zähler und Nenner der Näherungsbrüche.

I. Durch fortgesetzte Anwendung des in §. 3 erörterten Gesetzes ergibt sich für die Zähler und Nenner der Näherungsbrüche, ausgedrückt durch die Quotienten des Kettenbruchs:

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	a_0	a_0	1
1	a_1	$a_0 a_1 + 1$	a_1
2	a_2	$a_0 a_1 a_2 + a_0 + a_2$	$a_1 a_2 + 1$
3	a_3	$a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1$	$a_1 a_2 a_3 + a_1 + a_3$
4	a_4	$a_0 a_1 a_2 a_3 a_4 + a_0 a_1 a_2 + a_0 a_1 a_4 + a_0 a_3 a_4 + a_2 a_3 a_4 + a_0 + a_2 + a_4$	$a_1 a_2 a_3 a_4 + a_1 a_2 + a_1 a_4 + a_3 a_4 + 1$

u. s. w. Hieraus und aus der allgemeinen Rekursionsformel des §. 3 lassen sich leicht folgende Gesetze ableiten.

II. In den Zähler M_n treten die Quotienten a_0, a_1, a_2 . . . a_n ein und man hat

$$\begin{aligned} M_n = & (a_0 a_1 \ldots a_n) \\ & + (a_0 a_1 \ldots a_{n-2}) + \ldots + (a_2 a_3 \ldots a_n) \\ & + (a_0 a_1 \ldots a_{n-4}) + \ldots + (a_4 a_5 \ldots a_n) \\ & + (a_0 a_1 \ldots a_{n-6}) + \ldots + (a_6 a_7 \ldots a_n) \\ & + \text{etc.} \end{aligned}$$

Wenn n paar ist; so schliesst der Werth von M_n so:

$$\begin{aligned} & + \text{etc.} \\ & + (a_0 a_1 a_2) + \ldots + (a_{n-2} a_{n-1} a_n) \\ & + a_0 + a_2 + a_4 + \ldots + a_n \end{aligned}$$

Wenn n unpaar ist; so schliesst dieser Werth so:

$$\begin{aligned}&+ \text{etc.}\\ &+ (a_0\, a_1) + \ldots + (a_{n-1}\, a_n)\\ &+ 1\end{aligned}$$

Der Werth von M_n zerfällt in Kombinationen aus je n, $n-2$, $n-4$, . . . Quotienten. Wenn n paar; so enthält die letzte Klasse je Ein Element: wenn n unpaar; so enthält die letzte Klasse kein Element, sondern ist gleich 1. Eine jede Kombination beginnt mit einem Quotienten von paarem Zeiger, und die Zeiger zweier benachbarter Quotienten in einer Kombination fassen eine paare Menge von Zahlen zwischen sich (oder besitzen eine unpaare Differenz) wie z. B. in der Kombination $a_2\, a_3\, a_6\, a_7\, a_{12}$. Wenn man also die in einer Kombination aufeinander folgenden Zeiger betrachtet; so muss auf einen paaren stets ein unpaarer und auf einen unpaaren stets ein paarer folgen.

Nach diesem Gesetze sind alle möglichen Kombinationen aus a_0, a_1, a_2 . . . a_n zu bilden. Die Zusammenstellung erleichtert sich, wenn man die Quotienten in zwei Reihen unter einander schreibt, oben die mit paaren, unten die mit unpaaren Zeigern:

$$\begin{array}{cccccccccccc} a_0 & & a_2 & & a_4 & & a_6 & & a_8 & & \ldots & \\ & a_1 & & a_3 & & a_5 & & a_7 & & a_9 & & \ldots \end{array}$$

und nun abwechselnd Einen Quotienten aus der Einen und einen späteren Quotienten aus der anderen Reihe nimmt, wobei der erste Quotient stets aus der oberen Reihe zu nehmen ist.

Wenn der erste Quotient $a_0 = 0$ ist; so ändert sich das vorstehende Gesetz nicht. Es fallen dann alle mit a_0 anfangenden Kombinationen aus. Auch a_1 kann nun in keiner Kombination erscheinen.

III. In den Nenner N_n treten die Quotienten a_1, a_2, a_3 . . . a_n ein und man hat

$$\begin{aligned} N_n = {} & (a_1\, a_2 \ldots a_n)\\ & + (a_1\, a_2 \ldots a_{n-2}) + \ldots + (a_3\, a_4 \ldots a_n)\\ & + (a_1\, a_2 \ldots a_{n-4}) + \ldots + (a_5\, a_6 \ldots a_n)\\ & + (a_1\, a_2 \ldots a_{n-6}) + \ldots + (a_7\, a_8 \ldots a_n)\\ & + \text{etc.}\end{aligned}$$

Wenn n paar ist; so schliesst der Werth von N_n so:

$$\begin{aligned}&+ \text{etc.}\\ &+ (a_1\, a_2) + \ldots + (a_{n-1}\, a_n)\\ &+ 1\end{aligned}$$

Wenn n unpaar ist; so schliesst dieser Werth so:

$$+ \text{etc.}$$
$$+ (a_1 a_2 a_3) + \ldots + (a_{n-2} a_{n-1} a_n)$$
$$+ a_1 + a_3 + a_5 + \ldots + a_n$$

Der Werth von N_n zerfällt in Kombinationen aus je n-1, n-3, n-5 ... Quotienten. Wenn n paar; so enthält die letzte Klasse keinen Quotienten, sondern ist = 1: wenn n unpaar; so enthält die letzte Klasse je Einen Quotienten. Eine jede Kombination beginnt mit einem Quotienten von unpaarem Zeiger, und die Zeiger zweier benachbarter Quotienten in einer Kombination fassen eine paare Menge von Zahlen zwischen sich (oder besitzen eine unpaare Differenz) wie in der Kombination $a_1 a_4 a_7 a_{10} a_{11}$. Es müssen also stets paare Zeiger mit unpaaren abwechseln.

Behuf Bildung aller dieser Kombinationen kann man die beiden Reihen

$$\begin{array}{ccccccccccc} a_1 & & a_3 & & a_5 & & a_7 & & \ldots & & \\ & a_2 & & a_4 & & a_6 & & a_8 & & \ldots & \end{array}$$

schreiben und wie bei dem Zähler M_n verfahren. Der Quotient a_0 (d. i. die in dem Bruche K enthaltenen Ganzen) tritt niemals in die Werthe der Nenner N_n ein.

IV. In den beiden Kettenbrüchen $K = [a_0, a_1, a_2 \ldots]$ und $K' = [0, a_1, a_2 \ldots]$ welche in der Beziehung $K = a_0 + K'$ stehen, ist also $N_n = N_n'$, und aus dem obigen Bildungsgesetze folgt leicht $M_n = a_0 N_n + M_n' = a_0 N_n' + M_n'$.

Für die beiden Kettenbrüche $K = [a_0, a_1, a_2 \ldots]$ und $K'' = [a_1, a_2, a_3 \ldots]$, welche in der Beziehung $K = a_0 + \frac{1}{K''}$ stehen, so dass auch $K'' = \frac{1}{K'}$ ist, hat man $N_n = M''_{n-1}$ und $M_n = a_0 M''_{n-1} + N''_{n-1}$.

V. Wir werden in Zukunft einen nach dem independenten Bildungsgesetze erzeugten Werth von M_n oder N_n dadurch bezeichnen, dass wir unter dem allgemeinen Buchstaben a für die Quotienten den in der höchsten Kombinationsklasse vorkommenden kleinsten und grössten Zeiger, getrennt durch ein Komma, anmerken, und hiernach schreiben:

$$\begin{array}{ll} M_{-2} = 0 & N_{-2} = 1 \\ M_{-1} = 1 & N_{-1} = 0 \\ M_0 = a_0 & N_0 = 1 \\ M_1 = a_{0,1} & N_1 = a_1 \\ M_2 = a_{0,2} & N_2 = a_{1,2} \\ M_3 = a_{0,3} & N_3 = a_{1,3} \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ M_n = a_{0,n} & N_n = a_{1,n} \end{array}$$

VI. Das vorstehende independente Bildungsgesetz gibt Gelegenheit zu Untersuchungen über die Länge des aus dem gewöhnlichen Bruche $\frac{M}{N}$ entstehenden Kettenbruchs und über verwandte Dinge. Wir beschränken uns hier auf einige Andeutungen.

Als Kettenbruch mit einem einzigen Quotienten a_0 kann nur eine ganze Zahl sich darstellen; es muss also $N = 1$ sein.

In einem Kettenbruch mit zwei Quotienten a_0, a_1 kann ein Bruch mit beliebigem Nenner $N = a_1 > 1$ entwickelt werden, wenn der Zähler $M = a_0 a_1 + 1 = a_0 N + 1$ ein beliebiges Vielfaches des Nenners N, plus 1 ist; z. B. $\frac{16}{5} = \frac{3.5 + 1}{5}$.

In einen Kettenbruch mit drei Quotienten a_0, a_1, a_2 kann ebenfalls ein Bruch mit beliebigem Nenner $N = a_1 a_2 + 1$ entwickelt werden. Der Zähler $M = a_0 a_1 a_2 + a_0 + a_2 = a_0 N + a_2 = a_0 N + \frac{N - 1}{a_1}$ muss jedoch irgend ein Vielfaches des Nenners N, plus einem Faktor der Zahl $N - 1$ sein. Auch ist es nothwendig, dass dieser Faktor, welcher als a_2 den letzten Quotienten bildet, > 1 sei. Z. B. $\frac{37}{16} = \frac{2.16 + 5}{16}$.

Damit ein Kettenbruch mit vier oder mehr Quotienten erscheine, kann der Nenner N nicht mehr willkürlich sein. Derselbe muss vielmehr bei vier Quotienten der Form $a_1 a_2 a_3 + a_1 + a_3$ entsprechen, worin der letzte Quotient $a_3 > 1$ sein muss. Da hiernach $N - (a_1 + a_3) = a_1 a_2 a_3$ ist; so muss es zwei ganze Zahlen a_1, a_3, von denen die letztere > 1 ist, von der Beschaffenheit geben, dass wenn ihre Summe $a_1 + a_3$ von N subtrahirt wird, der Rest durch das Produkt $a_1 a_3$ jener bei-

den Zahlen theilbar bleibt. Dieser Bedingung entspricht jede unpaare Zahl, wenn man $a_1 = 1$, $a_3 = 2$ setzt, sowie jede paare Zahl, welche ein Vielfaches von 4 ist, wenn man $a_1 = 2$, $a_3 = 2$ setzt; nicht aber jede paare Zahl, welche kein Vielfaches von 4 ist. Unter den letzteren ist z. B. $14 = 2.1.4 + 2 + 4$ zulässig, nicht aber 6. Es kann also keinen Bruch vom Nenner 6 geben, welcher einen Kettenbruch mit 4 Quotienten lieferte.

Wenn es zwei Zahlen a_1, a_3 von der oben bezeichneten Art gibt; so muss der Zähler $M = a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1 = a_0 N + a_2 a_3 + 1 = a_0 N + \frac{N - a_3}{a_1}$ die durch den letzten Ausdruck dargestellte Form haben, worin a_0 willkürlich bleibt.

§. 13. *Umkehrung der Quotientenfolge.*

Wenn man die Reihenfolge der Quotienten in dem Kettenbruche $K = [a_0, a_1, a_2 \ldots a_n]$ umkehrt; so entsteht ein Kettenbruch, welchen wir mit $K' = [a'_0, a'_1, a'_2 \ldots a'_n] = [a_n, a_{n-1}, a_{n-2} \ldots a_0]$ bezeichnen wollen. Man erkennt aus dem Gesetze des vorhergehenden Paragraphen leicht, dass sich der Werth irgend einer Grösse M_n oder N_n nicht ändert, wenn man die Reihenfolge aller Quotienten $a_0, a_1 \ldots a_n$ umkehrt, indem $a_{0,n} = a_{n,0}$ und $a_{1,n} = a_{n,1}$ ist.

Demnach hat man

$$M_{n-1} = a_{0,n-1} \qquad N_{n-1} = a_{1,n-1}$$
$$M_n = a_{0,n} \qquad N_n = a_{1,n}$$
$$M'_{n-1} = a'_{0,n-1} = a'_{n-1,0} = a_{1,n} \qquad N'_{n-1} = a'_{1,n-1} = a'_{n-1,1} = a_{1,n-1}$$
$$M'_n = a'_{0,n} = a'_{n,0} = a_{0,n} \qquad N'_n = a'_{1,n} = a'_{n,1} = a_{0,n-1}$$

folglich bestehen die Beziehungen

$$M'_{n-1} = N_n \qquad N'_{n-1} = N_{n-1} \qquad \text{also } K'_{n-1} = \frac{M'_{n-1}}{N'_{n-1}} = \frac{N_n}{N_{n-1}}$$
$$M'_n = M_n \qquad N'_n = M_{n-1} \qquad K'_n = \frac{M'_n}{N'_n} = \frac{M_n}{M_{n-1}}$$

So hat man z. B. für

$K = [1, 3, 2, 1, 5]$ $\qquad$ $K' = [5, 1, 2, 3, 1]$

n	a_n	M_n	N_n	n	a'_n	M'_n	N'_n
−2		0	1	−2		0	1
−1		1	0	−1		1	0
0	1	1	1	0	5	5	1
1	3	4	3	1	1	6	1
2	2	9	7	2	2	17	3
3	1	13	10	3	3	57	10
4	5	74	57	4	1	74	13

Multiplizirt man M_r mit N_n und N_r mit M_n und subtrahirt diese Produkte; so ergibt sich unter Beachtung der Formeln in §. 4

(3) $$M_r\ N_n - M_n\ N_r = (-1)^n\ \mathfrak{N}_{r-n-1}$$

oder auch für $r = m + n$

(4) $$M_{m+n}\ N_n - M_n\ N_{m+n} = (-1)^n\ \mathfrak{N}_{m-1}$$

Hiernach ist, wenn man mit $N_n\ N_{m+n}$ dividirt, die Differenz zwischen irgend zwei Näherungsbrüchen

(5) $$\frac{M_{m+n}}{N_{m+n}} - \frac{M_n}{N_n} = K_{m+n} - K_n = (-1)^n\ \frac{\mathfrak{N}_{m-1}}{N_n\ N_{m+n}}$$

Wenn man in diesen Formeln für n das Zeichen $r-m$ an die Stelle, also

$$M_r\ N_{r-m} - M_{r-m}\ N_r = (-1)^{r-m}\ \mathfrak{N}_{m-1}$$

$$K_r - K_{r-m} = (-1)^{r-m} \frac{\mathfrak{N}_{m-1}}{N_{r-m}\ N_r}$$

setzen will; so muss man beachten, dass dann

$$\mathfrak{K} = [a_{r-m+1},\ a_{r-m+2} \ldots a_r] \text{ ist.}$$

Aus den letzten Formeln erkennt man, wenn man beachtet, dass $\mathfrak{N}_{m-1}$ umso grösser und N_{r-m} umso kleiner ist, je grösser m ist, dass nicht bloss der absolute Werth von $K_r - K_{r-m}$, sondern auch der von $M_r\ N_{r-m} - M_{r-m}\ N_r$ umso grösser ausfällt, je kleiner bei konstantem r der frühere Zeiger $r-m$ genommen wird.

§. 16. *Beziehung zwischen den Näherungs- oder Mittelbrüchen und der Lehre vom Grössten und Kleinsten in ganzen Zahlen.*

Wir machen noch auf folgende wichtige Beziehungen aufmerksam.

I. Wenn K_n irgend ein Näherungsbruch von K ist, und man bezeichnet den absoluten Werth der Differenz

(1) $$X = K_n - K = \frac{M_n}{N_n} - \frac{M}{N}$$

mit X'; so leuchtet aus §. 7 ein, dass wenn man in vorstehender Gleichung für K_n einen anderen Bruch mit kleinerem Zähler, oder Nenner, oder Zähler und Nenner setzt, der Werth X' jener Differenz stets grösser wird.

Diese Behauptung behält nach §. 8 auch dann noch volle Gültigkeit, wenn K_n ein Mittelbruch von K ist.

Ferner behaupten wir, dass wenn L weder ein Näherungs-, noch ein Mittelbruch von K ist, es immer einen Bruch mit kleinerem Zähler und Nenner gibt, welcher, wenn er für L gesetzt wird, den Betrag X' der Differenz $L-K$ verkleinert.

Um Dies einzusehen, braucht man nur die Mittelbrüche ins Auge zu fassen, da nach §. 9 die Näherungsbrüche selbst wie Mittelbrüche angesehen werden können. Da unter den Näherungsbrüchen stets die Grössen $0 = K_{-2}$ und $\infty = \frac{1}{0} = K_{-1}$ vorkommen; so muss es stets zwei benachbarte Mittelbrüche $K_p^{(n)}$ und $K_{p+1}^{(n)}$ geben, zwischen welchen der Werth von L liegt. Von diesen beiden Mittelbrüchen liegt der zweite näher als der erste und auch näher als L an K. Derselbe besteht zwar aus grösseren Zahlen als der erste, aber nach §. 8 aus kleineren Zahlen als L. Demnach kann L durch einen Bruch $K_{p+1}^{(n)}$ ersetzt werden, welcher aus kleineren Zahlen besteht und die Differenz X' vermindert.

II. Will man also in der Gleichung

(2) $$X = \frac{x}{y} - \frac{a}{b}$$

worin $\frac{a}{b}$ gegeben ist, den Bruch $\frac{x}{y}$ so bestimmen, dass der absolute Betrag X' von X sich immer vermehrt, wenn man x oder y oder Beide vermindert; so sind die nach §. 9 leicht darzustellenden Mittelbrüche von $\frac{a}{b}$ (mit Einschluss der Näherungsbrüche) die gesuchten Werthe von $\frac{x}{y}$ und sonst keine.

III. Multipliziren wir jetzt den Werth von X in Gl. (1) mit N_n und schreiben wir

(3) $$Y = N_n(K_n - K) = N_n\left(\frac{M_n}{N_n} - \frac{M}{N}\right) = M_n - \frac{M}{N}N_n$$

oder auch

(4) $$NY = NM_n - MN_n$$

so lässt sich behaupten, dass wenn man für M_n oder N_n oder für Beide kleinere Zahlen setzt, der absolute Werth Y' von Y in Gl. (3), also auch der von NY' in Gl. (4) sich vergrössert oder wenigstens derselbe bleibt.

Dieser Satz gilt jedoch nur von den Näherungsbrüchen $\frac{M_n}{N_n}$ und nicht von den Mittelbrüchen, indem sich, wenn $\frac{M_n}{N_n}$ ein Mittelbruch oder ein beliebiger anderer Bruch ist, für M_n oder N_n oder für Beide stets kleinere Werthe setzen lassen, wodurch auch Y' kleiner wird.

Wir beweisen den letzteren Theil dieser Behauptung zuerst. Wäre $\frac{P}{Q}$ kein Näherungs- und kein Mittelbruch, und $NY =$

$NP - MQ$; so liege $\frac{P}{Q}$ zwischen den beiden benachbarten Mittelbrüchen $K_p^{(n)}$ und $K_{p+1}^{(n)}$. Der letztere dieser beiden Mittelbrüche hat nicht allein kleinere Zahlen als $\frac{P}{Q}$, sondern liegt auch näher an K. Nimmt man also dessen Zähler statt P und dessen Nenner statt Q; so vermindert sich $\frac{P}{Q} - \frac{M}{N}$, und gleichzeitig vermindert sich Q oder bleibt ungeändert. Es vermindert sich also entschieden der Werth von NY'.

Wäre $\frac{P}{Q}$ ein Mittelbruch $K_p^{(n)}$, welcher zwischen den beiden Näherungsbrüchen K_n und K_{n+2} eingeschaltet ist; so besitzt bekanntlich der Näherungsbruch K_{n+1} kleinere Zahlen, als jener Mittelbruch, liegt aber auf entgegengesetzter Seite von K (§. 8). Setzt man nun Zähler und Nenner des aus kleineren Zahlen bestehenden Näherungsbruchs K_{n+1} für den Zähler und Nenner des Mittelbruchs $\frac{P}{Q}$; so vermindert sich der Werth von $NP - MQ$, denn man hat (ohne Rücksicht auf das Zeichen)

$$NM_{n+1} - MN_{n+1} < NP - MQ \text{ oder}$$

$$N_{n+1}\left(\frac{M_{n+1}}{N_{n+1}} - \frac{M}{N}\right) < Q\left(\frac{P}{Q} - \frac{M}{N}\right) \text{ oder}$$

$$N_{n+1}(K_{n+1} - K) < N_p^{(n)}(K_p^{(n)} - K).$$

Die Richtigkeit der letzten Formel leuchtet ein, wenn man darin nach §. 6 den absoluten Werth von

$$K_{n+1} - K = \frac{x_{n+1}}{N_{n+1}(N_{n+1} + N_n x_{n+1})}$$

und nach §. 8 den absoluten Werth von

$$K_p^{(n)} - K = \frac{1 - p x_{n+1}}{N_p^{(n)}(N_{n+1} + N_n x_{n+1})}$$

setzt. Denn jetzt braucht nur gezeigt zu werden, dass

$$x_{n+1} < 1 - p x_{n+1} \text{ oder } (p+1) x_{n+1} < 1$$

oder weil $x_{n+1} = \frac{1}{a_{n+2} + x_{n+2}}$ ist, dass

$$p + 1 < a_{n+2} + x_{n+2} \text{ oder } p < a_{n+2} - 1 + x_{n+2}$$

oder da p nur eine ganze Zahl und x_{n+2} nicht grösser als 1 sein kann, dass $p < a_{n+2}$ sei. Diese letztere Bedingung ist aber für jeden zwischen K_n und K_{n+2} liegenden Mittelbruch wirklich erfüllt.

Hiernach bleiben nur noch die eigentlichen Näherungsbrüche von $\frac{M}{N}$ zu betrachten. Von jedem derselben wie $\frac{M_n}{N_n}$ lässt sich behaupten, dass wenn man statt M_n oder N_n oder für Beide kleinere Zahlen P, Q setzt, der Werth von Y' und auch der von NY' sich vergrössere.

Denn angenommen P, Q lieferte einen kleineren Werth für NY'. Ist nun $\frac{P}{Q}$ nicht genau ein früherer Näherungsbruch $\frac{M_{n-m}}{N_{n-m}}$ von $\frac{M}{N}$; so lässt sich nach Obigem P, Q noch weiter verkleinern, sodass NY' noch kleiner wird, als zuvor. Dieser Schluss kann so lange fortgesetzt werden, bis man auf irgend einen früheren Näherungsbruch $\frac{M_{n-m}}{N_{n-m}}$ stösst. Hierin liegt aber ein Widerspruch gegen das letzte Ergebniss des vorhergehenden Paragraphen, indem für einen solchen früheren Näherungsbruch der absolute Betrag von

$$NM_{n-m} - MN_{n-m} \text{ nicht } <, \text{ sondern } > NM_n - MN_n$$

ist. Demnach kann aus einer Verkleinerung der Zahlen M_n, N_n nur eine Vergrösserung oder ein Konstantbleiben von Y' und NY' hervorgehen.

IV. Will man also in der Gleichung

$$(5) \qquad Y = y\left(\frac{x}{y} - \frac{a}{b}\right) = x - \frac{a}{b}y$$

oder auch in der Gleichung

$$(6) \qquad bY = bx - ay$$

worin a und b gegeben sind, die ganzen Zahlen x und y so bestimmen, dass mit einer Verkleinerung der Einen oder der anderen oder Beider eine Vergrösserung oder wenigstens ein Konstantbleiben des absoluten Werthes Y' von Y verbunden ist; so sind die Näherungsbrüche von $\frac{a}{b}$ die gesuchten Werthe von $\frac{x}{y}$ und sonst keine.

§ 17. *Kettenbrüche mit positiven und negativen Quotienten.*

Lassen wir jetzt unter den Quotienten eines Kettenbruchs auch negative Zahlen, sowie die Zahl null zu; so behalten offenbar die Formeln und Gesetze der §§. 2 bis 5 und 12 bis 15 (mit Ausnahme des Schlusssatzes in §. 15) vollkommene Gültigkeit.

So hat man z. B. für $K = [1, 3, -2, 4, 0, 5]$ folgende Reduktion

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	3	4	3
2	-2	-7	-5
3	4	-24	-17
4	0	-7	-5
5	5	-59	-42

also $K = \frac{-59}{-42} = \frac{59}{42}$

und für $K = [-3, 2, -1]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	-3	-3	1
1	2	-5	2
2	-1	2	-1

also $K = \frac{2}{-1} = -2$

Wesentlich ist, dass auch bei ganz beliebigen Quotienten Zähler und Nenner eines Näherungsbruches stets relativ prim sind. Im Übrigen sind hier die Fehlergränzen im Allgemeinen sehr ausgedehnt.

§. 18. *Entwickelung eines gemeinen Bruches in einen Kettenbruch mit willkürlichen Quotienten.*

I. Kettenbrüche dieser Art ergeben sich, wenn man bei dem Divisionsverfahren behuf Verwandlung eines gemeinen Bruches in einen Kettenbruch von dem Prinzipe der grössten Subquotienten (§. 10) in der Weise abweicht, dass man an dieser oder jener Stelle einen kleineren oder grösseren Quotienten willkürlich annimmt. Wollte man in dieser willkürlichen Weise ununterbrochen fortfahren; so würde die Entwickelung endlos sein. Es leuchtet jedoch ein, dass man an jeder Stelle der Rechnung zu dem Prinzipe der grössten Subquotienten zurückkehren, und danach jede noch so willkürlich angefangene Entwickelung eines Bruches K zum Schlusse bringen kann.

Hierbei bemerken wir, dass wenn von Divisor und Dividend Einer oder Beide das negative Zeichen haben, wir immer unter einem Subquotienten einen solchen verstehen, für welchen der Restbruch positiv, dagegen unter einem Superquotienten einen solchen, für welchen der Restbruch negativ wird, ganz nach §. 10. Wenn demnach M und N positiv sind, ferner x und $y = 1 - x$ zwei positive Grössen < 1 bezeichnen und

für grösste Subq. $\frac{M}{N} = a + x$ — für kleinste Superq. $\frac{M}{N} = (a+1) - y$

ist; so hat man

für grösste Subq. $-\frac{M}{N} = -(a+1) + y$ — für kleinste Superq. $-\frac{M}{N} = -a - x$

Im nachstehenden Beispiele für $K = \frac{13}{4}$ ist die Entwickelung bis zum Quotienten $a_2 = -3$ willkürlich, später aber streng nach dem Prinzipe der grössten Subquotienten geführt.

$$
\begin{array}{l}
4 \mid 13 \mid 2 \\
\quad\; 8 \\
\overline{5} \mid 4 \mid 1 \\
\quad\; 5 \\
\overline{-1} \mid 5 \mid -3 = a_2 \\
\quad\; 3 \\
2 \mid -1 \mid -1 \\
\quad\; -2 \\
\overline{1} \mid 2 \mid 2 \\
\quad\; 2 \\
\overline{0}
\end{array}
$$

also $\frac{13}{4} = [2, 1, -3, -1, 2]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	2	2	1
1	1	3	1
2	-3	-7	-2
3	-1	10	3
4	2	13	4

II. Wenn man in einer solchen Entwickelung nur Ein Mal (etwa bei a_n) von dem Prinzipe der grössten Subquotienten abweicht; so wird, wenn man statt des grössten Subquotienten a_n den Werth $a_n - p$ nimmt, worin p irgend eine positive Zahl bezeichnen soll, $a_{n+1} = 0$ und alle folgenden Quotienten > 0 werden: wenn man dagegen statt a_n den Werth $a_n + p$ nimmt; so wird a_{n+1} negativ, also < 0, und alle folgenden Quotienten > 0 werden.

III. Bei Zulassung negativer Quotienten kann man bewirken, dass mehrere beliebig gegebene Brüche $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \ldots$ (oder auch ganze Zahlen, welche Brüche mit dem Nenner 1 sind) als Näherungswerthe Ein und desselben Kettenbruchs erscheinen. Um Dies zu bewirken, entwickelt man zuerst den Bruch $\frac{a}{b}$ nach dem Prinzipe der grössten Subquotienten. Darauf geht man an die Entwickelung von $\frac{c}{d}$, nimmt aber die Quotienten von $\frac{a}{b}$ als willkürlichen Anfang der Entwickelung von $\frac{c}{d}$, und führt darauf die letztere Entwickelung nach dem Prinzipe der grössten Subquotienten zum Schlusse. Hierauf entwickelt man $\frac{e}{f}$, schickt dabei

nur die Quotienten der eben erwähnten Entwickelung von $\frac{c}{d}$ als willkürlichen Anfang voraus, u. s. w.

Sollten z. B. der Reihe nach die Zahlen $\frac{2}{3}$, 7, $\frac{1}{5}$ als Näherungswerthe eines Kettenbruchs erscheinen; so hat man

```
3|2|0        1|7|0                    5|1|0
  0            0                        0
 2|3|1        7|1|1                    1|5|1
   2            7                         1
  1|2|2       -6|7|2                   4|1|2
    2            -12                      8
    0          19|-6|-1                -7|4|-1
                  -19                       7
                13|19|1                 -3|-7|1
                   13                      -3
                  6|13|2                 -4|-3|2
                     12                     -8
                    1|6|6                  5|-4|6
                      6                       30
                      0                   -34|5|-1
                                               34
                                            -29|-34|1
                                                 -29
                                               -5|-29|5
                                                   -25
                                                 -4|-5|1
                                                    -4
                                                   -1|-4|4
                                                      -4
                                                       0
```

Der gesuchte Kettenbruch ist also

$$K = [0, 1, 2, -1, 1, 2, 6, -1, 1, 5, 1, 4]$$

n	a_n	M_n	N_n	
-2		0	1	
-1		1	0	
0	0	0	1	
1	1	1	1	
2	2	2	3	$K_2 = \frac{2}{3}$
3	-1	-1	-2	
4	1	1	1	
5	2	1	0	
6	6	7	1	$K_6 = \frac{7}{1} = 7$
7	-1	-6	-1	
8	1	1	0	
9	5	-1	-1	
10	1	0	-1	
11	4	-1	-5	$K_{11} = \frac{-1}{-5} = \frac{1}{5}$

IV. Wir machen noch auf folgende Beziehung aufmerksam. Wenn man auf den letzten Quotienten des Kettenbruchs $[a_0, a_1 \dots a_n]$ erst den Quotienten 0 und dann die vorstehenden Quotienten in umgekehrter Ordnung und mit entgegengesetzten Zeichen folgen lässt, also den Kettenbruch

$$[a_0 \dots a_{n-1}, a_n, 0, -a_n, -a_{n-1} \dots -a_0]$$

bildet; so werden sich bei dieser Fortsetzung des gegebenen Kettenbruchs die Zähler und Nenner der Näherungsbrüche desselben in umgekehrter Reihenfolge wiederholen.

So hat man z. B. für den Kettenbruch [2, 1, 3, 0, -3, -1, -2], welcher nach Vorstehendem die Fortsetzung des Kettenbruchs [2, 1, 3] bildet,

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	2	2	1
1	1	3	1
2	3	11	4
3	0	3	1
4	-3	2	1
5	-1	1	0
6	-2	0	1

Allgemein erkennt man, dass

$$[a_0, \dots a_n, 0, -a_n \dots -a_{n-r}] = [a_0, \dots a_{n-r-2}]$$

ist, auch dass der Gesammtwerth eines Kettenbruchs unverändert bleibt, wenn man an denselben noch eine Quotientenfolge wie

$$a_{n+1}, a_{n+2} \dots a_{n+r-1}, a_{n+r}, 0, -a_{n+r}, -a_{n+r-1} \dots -a_{n+2}$$

anhängt.

§. 19. *Entwickelung eines negativen Bruches in einen Kettenbruch mit grössten Subquotienten.*

I. Wenn man einen negativen Bruch nach dem eben genannten Prinzipe in einen Kettenbruch verwandelt; so ist die Rechnung an keiner Stelle willkürlich. Es leuchtet ein, dass der erste Quotient a_0 entschieden negativ, alle folgenden aber positiv > 0 werden müssen. Z. B. $K = -\frac{51}{20}$

```
20|-51|-3
  |-60|
   9|20|2
    |18|
     2|9|4
      |8|
      1|2|2
       |2|
        0
```

also $-\frac{51}{20} = [-3, 2, 4, 2]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	-3	-3	1
1	2	-5	2
2	4	-23	9
3	2	-51	20

Da der Quotient $a_0 = -a$ in die Nenner N nicht eintritt; so ist klar, dass dieselben stets positiv ausfallen werden. Was jedoch die Zähler anlangt; so hat man $M_0 = a_0 = -a$, $M_1 = a_0 a_1 + 1 = -(a a_1 - 1)$. Hieraus ist klar, dass alle Zähler negativ sein werden, und dass sich nur der einzige M_1 für den besonderen Fall $a_0 = -1$, $a_1 = 1$ bis auf null erheben kann.

II. Man kann übrigens unbeschadet aller bisherigen Gesetze die Zeichen der Zähler und Nenner aller Näherungsbrüche in die entgegengesetzten verwandeln, wodurch im vorstehenden Falle die Zähler positiv und die Nenner negativ werden würden. Wenn man diese Beziehung gleich von vorn herein beabsichtigte; so braucht man nur die Zeichen der Zähler und Nenner der beiden fingirten Näherungsbrüche $K_{-2} = \frac{0}{1}$ und $K_{-1} = \frac{1}{0}$ umzukehren, also $K_{-2} = \frac{0}{-1}$ und $K_{-1} = \frac{-1}{0}$ zu schreiben. Dies würde in dem obigen Beispiele geben

n	a_n	M_n	N_n
-2		0	-1
-1		-1	0
0	-3	3	-1
1	2	5	-2
2	4	23	-9
3	2	51	-20

Diese Substitution von -1 statt 1 für N_{-2} und M_{-1} kann man auch dann anwenden, wenn Zähler und Nenner des entwickelten Bruches beide negativ sind, um hierdurch eben solche Näherungsbrüche zu erhalten. Z. B. als Entwickelung von $K = \frac{-16}{-5} = [3, 5]$

n	a_n	M_n	N_n
-2		0	-1
-1		-1	0
0	3	-3	-1
1	5	-16	-5

§. 20. *Entwickelung eines Bruches in einen Kettenbruch mit kleinsten Superquotienten.*

I. Wenn man bei der Kettenbruchsentwickelung das Prinzip der kleinsten Superquotienten zu Grunde legt; so leuchtet ein, dass alsdann die Rechnung ebenso wie bei dem Prinzipe der grössten Subquotienten vollkommen bestimmt ist. Wenn Zähler und Nenner des zu entwickelnden Bruches gleiche Zeichen haben; so werden die Quotienten negativ, mit Ausnahme des ersten a_0, welcher positiv und >0 wird: wenn dieselben je-

doch ungleiche Zeichen haben; so werden alle Quotienten negativ, indem der erste a_0 höchstens bis null ansteigen kann. Da der absolute Werth jedes Restes kleiner ist, als der vorhergehende Divisor; so leuchtet ein, dass die Rechnung stets nur eine endliche Länge besitzen kann. Z. B.

$$K = \frac{11}{15} = [1, -3, -1, -3]$$

```
15|11|1
   15
  -4|15|-3
     12
     3|-4|-1
       -3
       -1|3|-3
          3
          0
```

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	-3	-2	-3
2	-1	3	4
3	-3	-11	-15

$$K = -\frac{48}{13} = [-3, -1, -2, -4]$$

```
13|-48|-3
   -39
    -9|13|-1
        9
        4|-9|-2
          -8
          -1|4|-4
              4
              0
```

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	-3	-3	1
1	-1	4	-1
2	-2	-11	3
3	-4	48	-13

II. Man erkennt leicht, dass die kleinsten Superquotienten eines negativen Bruches $-K$ die negativen Werthe der grössten Subquotienten des positiven Bruches K sind.

Allgemein erhellet, dass wenn $K = [a_0, a_1, a_2 \ldots]$ und bei Umkehrung der Zeichen aller Quotienten $K' = [-a_0, -a_1, -a_2 \ldots] = [a'_0, a'_1, a'_2 \ldots]$ ist, nach dem independenten Gesetze des §. 12

$M_n = a_{0,n}$ $\qquad$ $N_n = a_{1,n}$

$M'_n = a'_{0,n} = (-1)^{n+1} a_{0,n}$ $\qquad$ $N'_n = a'_{1,n} = (-1)^n a_{1,n}$ also

$M'_n = (-1)^{n+1} M_n$ $\qquad$ $N'_n = (-1)^n N_n$ $\qquad$ $K'_n = -K_n$

ist. Es werden daher alle Zähler und Nenner der Näherungsbrüche von K' die absoluten Werthe der entsprechenden Grössen aus K haben, jedoch abwechselnd mit denselben und entgegengesetzten Zeichen. Aus diesem Umstande erkennt man, dass für die Näherungsbrüche eines Kettenbruches mit lauter negativen Quotienten auch die in §. 6 und 7 über Fehler-

gränzen und relative Kleinheit der Zahlen für Kettenbrüche mit lauter positiven Quotienten entwickelten Gesetze Gültigkeit haben.

§. 21. ***Entwickelung eines Bruches in einen Kettenbruch mit numerisch grössten Subquotienten.***

I. Wenn in $K=\frac{M}{N}$ M und N gleiche Zeichen haben, also K positiv ist; so sind die grössten Subquotienten sämmtlich positiv, und wenn M und N ungleiche Zeichen haben, also K negativ ist; so sind die kleinsten Superquotienten sämmtlich negativ. Es ist also in den Fällen, wo die Gültigkeit aller Fundamentalgesetze, namentlich derjenigen über die Fehlergränzen und die relative Kleinheit der Zahlen, wünschenswerth erscheint, rathsam, die positiven Brüche mit grössten Subquotienten, und die negativen Brüche mit kleinsten Superquotienten zu entwickeln.

Nun ist klar, dass wenn bei irgend einer Division der Divisor und der Dividend gleiche Zeichen haben, der grösste Subquotient auch immer diesen Namen verdient, selbst wenn man nur den numerischen Werth des Divisors und Dividends ins Auge fasst, und dass wenn der Divisor und der Dividend ungleiche Zeichen haben, der kleinste Superquotient bei blosser Berücksichtigung des numerischen Zahlwerthes des Divisors und Dividends, ebenfalls der grösste Subquotient ist.

Demnach braucht man, um den obigen Zweck zu erreichen, gleichviel, ob K positiv oder negativ ist, immer nur die numerisch grössten Subquotienten auszuwerfen, indem man jedoch unter allen Umständen das Zeichen nach den bekannten Regeln der Division bestimmt.

Diese Thatsache ist von Wichtigkeit, weil sie den Gedanken während der Rechnung von der lästigen Berücksichtigung vielfacher Modalitäten befreit.

II. Schliesslich wird noch erinnert, dass der reduzirte Kettenbruch oder der letzte Näherungsbruch desselben, wenn man $N_{-2}=1$ und $M_{-1}=1$ genommen hat, sowol für $\frac{+M}{+N}$ als auch für $\frac{-M}{-N}$ stets in der Form $\frac{+M}{+N}$, dagegen für $\frac{+M}{-N}$ und auch für $\frac{-M}{+N}$ bald in der Form $\frac{+M}{-N}$, bald in der Form $\frac{-M}{+N}$ erscheint. Will man die nicht erscheinende Form erzeugen; so braucht man nach geschehener Reduction nur die Zeichen der Zähler und Nenner aller Näherungswerthe umzukehren.

So hat man z. B. für $-\frac{48}{13} = [-3, -1, -2, -4]$

ebensowol:

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	-3	-3	1
1	-1	4	-1
2	-2	-11	3
3	-4	48	-13

als auch:

n	a_n	M_n	N_n
-2		0	-1
-1		-1	0
0	-3	3	-1
1	-1	-4	1
2	-2	11	-3
3	-4	-48	13

§. 22. *Entwickelung eines Bruches in einen Kettenbruch mit numerisch kleinsten Resten.*

I. Es leuchtet ein, dass wenn in der Formel

$$(1) \qquad \frac{M}{N} = a + \frac{R}{N} = b + \frac{S}{N}$$

a den grössten Sub- und b den kleinsten Superquotienten von $\frac{M}{N}$ bezeichnet, für die numerischen Werthe der beiden Reste R und S nothwendig Eine der drei nachfolgenden Beziehungen stattfinden muss

$$(2) \qquad R < \frac{1}{2} N, \qquad S > \frac{1}{2} N$$

$$(3) \qquad R > \frac{1}{2} N, \qquad S < \frac{1}{2} N$$

$$(4) \qquad R = \frac{1}{2} N, \qquad S = \frac{1}{2} N$$

Man kann also den Quotienten stets so wählen (entweder als grössten Sub- oder als kleinsten Superquotienten), dass der numerische Werth des Restes $\leqq \frac{1}{2} N$ ist.

Eine Entwicklung dieser Art ist besonders darum von Interesse, weil in derselben die nach und nach auftretenden Reste im Allgemeinen die am stärksten convergirende Reihe bilden, also in den meisten Fällen den Kettenbruch von kleinstmöglicher Länge ergeben. Durch dieses Verfahren wird denn auch die Aufsuchung des grössten gemeinschaftlichen Maasses zwischen zwei Zahlen M, N in der Regel die geringste Rechnung erfordern.

So hat man z. B., um den Bruch $\frac{38}{14}$ in einen Kettenbruch zu verwandeln, oder um das grösste gemeinschaftliche Maass von 38 und 14 zu ermitteln,

bei grössten Subquotienten: | bei numerisch kleinsten Resten:

14 | 38 | 2		0	1	14 | 38 | 3		0	1
28		1	0	42		1	0
10 | 14 | 1	2	2	1	−4 | 14 | −3	3	3	1
10	1	3	1	12	−3	−8	−3
4 | 10 | 2	2	8	3	2 | −4 | −2	−2	19	7
8	2	19	7	−4			
2 | 4 | 2				0			
4							
0							

Im zweiten Falle sind also nur drei Divisionen und Quotienten zu bilden, während man im ersten Falle deren vier darzustellen hat.

Es lassen sich leicht die Gränzen angeben, welche der 1., 2., 3., . . . Rest, sowie auch der 1., 2., 3., . . . Quotient bei der vorstehenden Kettenbruchsentwickelung, numerisch genommen, nicht übersteigen können. Man hat nämlich, wenn man folgende Bezeichnung

(5) $M = a_0 N + R_1, \quad N = a_1 R_1 + R_2, \quad R_1 = a_2 R_2 + R_3$ etc.

zu Grunde legt, und a_n der letzte Quotient, also R_n der letzte Divisor und $R_{n+1} = 0$ ist,

$$\begin{array}{ll|l}
 & R_1 < \frac{1}{2} N & a_0 \leqq M \\
 & R_2 < \frac{1}{2} R_1 < \frac{1}{4} N & a_1 < \frac{1}{2} N \\
 & R_3 < \frac{1}{2} R_2 < \frac{1}{8} N & a_2 < \frac{1}{2} R_1 < \frac{1}{4} N \\
 & \cdot & a_3 < \frac{1}{2} R_2 < \frac{1}{8} N \\
 & \cdot & \cdot \\
 & \cdot & \cdot \\
 & R_{n-1} < \frac{1}{2} R_{n-2} < \frac{1}{2^{n-1}} N & \cdot \\
 & & a_{n-1} \leqq \frac{1}{2} R_{n-2} \leqq \frac{1}{2^{n-1}} N \\
(6) & R_n \leqq \frac{1}{2} R_{n-1} \leqq \frac{1}{2^n} N & a_n \leqq R_{n-1} \leqq \frac{1}{2^{n-1}} N
\end{array}$$

Es ist klar, dass R_n jedenfalls dann der letzte Divisor sein wird, wenn sein Betrag < 2, also $= 1$ ist. Demnach muss vermöge der vorstehenden Beziehung (6)

(7) $$\frac{1}{2^n} N \geqq 2 \text{ oder } 2^{n+1} \leqq N$$

sein, wobei jedoch $n > 0$ vorausgesetzt wird. Hierin bezeichnet $n + 1$ die Anzahl der Quotienten $a_0, a_1 \ldots a_n$ des Ketten-

bruchs, welcher $= \frac{M}{N}$ ist. Man erkennt also, dass die Kettenbruchsentwickelung mit numerisch kleinsten Resten von einem Bruche, dessen Nenner

$N \leqq$ 4	ist,	höchstens	2	Quotienten
8	»	»	3	»
16	»	»	4	»
32	»	»	5	»
64	»	»	6	»
128	»	»	7	»
256	»	»	8	»
512	»	»	9	»
1024	»	»	10	»

u. s. w. besitzen kann.

III. Es ist noch zu beachten, dass weil vom Divisor R_1 an jeder Divisor $\leqq$ dem halben Dividende ist, ein jeder Quotient von a_1 an $\geqq$ 2 sein muss.

Aus dieser Beziehung und den bekannten Formeln $M_n = a_n M_{n-1} + M_{n-2}$ und $N_n = a_n N_{n-1} + N_{n-2}$ folgt, dass sowol die Zähler, wie die Nenner der aufeinander folgenden Näherungsbrüche numerisch **stets grösser** werden, wenigstens dass niemals ein späterer Zähler oder Nenner kleiner sein kann, als ein früherer. Denn wenn dieses Gesetz bis zum Zeiger $n-1$ gilt, wenn also numerisch $M_{n-1} \geqq \pm M_{n-2}$ ist; so gilt es auch für den nächstfolgenden Zeiger, weil nun $2\,M_{n-1} \geqq M_{n-1} \pm M_{n-2}$, also noch weit eher $a_n M_{n-1} \geqq M_{n-1} \pm M_{n-2}$ oder $a_n M_{n-1} \mp M_{n-2} \geqq M_{n-1}$ d. i. $M_n \geqq M_{n-1}$ ist. Jenes Gesetz kann aber leicht für die Zeiger 0 und 1 dargethan werden; es gilt mithin allgemein.

Aus diesem fortwährenden Wachsthume der Zähler und Nenner der Näherungsbrüche folgt auch, dass die Werthe der Grössen $\frac{1}{N_n}$ mit wachsendem Zeiger n immer kleiner werden. Demnach erkennt man aus den Formeln des §. 6, dass der Unterschied zwischen je zwei benachbarten Näherungsbrüchen oder zwischen einem Näherungsbruche und dem Gesammtwerthe des ganzen Kettenbruchs immer mehr abnimmt, je höher die Zeiger der Näherungsbrüche genommen werden.

§. 23. *Kettenbrüche nach dem Subtraktionsprinzipe.*

I. Gleichviel, ob die Quotienten a_0, a_1 . . . eines Kettenbruchs positiv oder negativ waren, immer haben wir bisher vorausgesetzt, dass die Glieder des Kettenbruchs durch Addition verbunden seien. Jetzt wollen wir zur Betrachtung solcher übergehen, in welchen die Glieder durchgängig durch Subtraktion verknüpft sind, wie in

$$a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{a_3 - \text{etc.}}}}$$

wobei ebenfalls die Quotienten $a_0, a_1, a_2 \ldots$ positiv und negativ sein können. Wäre der erste Quotient $a_0 = 0$; so stände vor dem eigentlichen Kettenbruche das Zeichen —, wie bei

$$-\cfrac{1}{a_1 - \cfrac{1}{a_2 - \text{etc.}}}$$

Wenn es darauf ankommt, diese beiden Arten zu unterscheiden; so werden wir die erstere Kettenbrüche nach dem Additionsprinzipe nennen und mit $K(+) = [a_0, a_1, a_2 \ldots] (+)$ bezeichnen: dagegen werden wir die letztere Kettenbrüche nach dem Subtraktionsprinzipe nennen und mit $K(-) = [a_0, a_1, a_2 \ldots] (-)$ bezeichnen.

Reden wir jetzt ausschliesslich von der letzteren Art. Bei einer leicht verständlichen Übertragung der früheren Bezeichnungsweise auf die gegenwärtigen Zahlformen findet man in einer der Entwickelung des §. 3 ähnlichen Weise folgendes Rekursionsgesetz für die Zähler und Nenner der Näherungsbrüche

(1) $M_n = a_n M_{n-1} - M_{n-2} \qquad N_n = a_n N_{n-1} - N_{n-2}$

Ausserdem hat man

(2) $$K = \frac{M_n - M_{n-1} x_n}{N_n - N_{n-1} x_n}\,,$$

worin $x_n = \cfrac{1}{a_{n+1} - x_{n+1}} = \cfrac{1}{a_{n+1} - \cfrac{1}{a_{n+2} - \text{etc.}}}$ ist.

II. Damit diese Gesetze schon für den Zeiger $n = 0$ Gültigkeit erlangen, muss man hier die Grössen

$$M_{-2} = 0 \qquad N_{-2} = -1$$
$$M_{-1} = 1 \qquad N_{-1} = 0$$

fingiren. Alsdann kann man die Reduktion eines Kettenbruchs nach einem dem früheren ähnlichen Schema ausführen. So hat man z. B.

für $K(-) = [3, 5, 1, 4] (-)$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	3	3	1
1	5	14	5
2	1	11	4
3	4	30	11

für $K(-) = [0, 5, 1, 4] (-)$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	0	0	1
1	5	-1	5
2	1	-1	4
3	4	-3	11

multiplizirt, $= -\cfrac{1}{-a-\cfrac{1}{b}}$ geschrieben werden kann. Hiernach hat man offenbar

$$[a_0, a_1, a_2, a_3, a_4, a_5 \ldots] (+) = [a_0, -a_1, a_2, -a_3, a_4, -a_5 \ldots] (-)$$

und

$$[a_0, a_1, a_2, a_3, a_4, a_5 \ldots] (-) = [a_0, -a_1, a_2, -a_3, a_4, -a_5 \ldots] (+)$$

Kehrt man also die Zeichen aller Quotienten mit unpaaren Zeigern um; so geht der gegebene Kettenbruch von der Einen Art in einen ihm gleichen von der anderen Art über. So hat man z. B.

$$[2, 4, -3, -1, 5] (+) = [2, -4, -3, 1, 5] (-)$$

n	a_n	M_n	N_n	n	a_n	M_n	N_n
-2		0	1	-2		0	-1
-1		1	0	-1		1	0
0	2	2	1	0	2	2	1
1	4	9	4	1	-4	-9	-4
2	-3	-25	-11	2	-3	25	11
3	-1	34	15	3	1	34	15
4	5	145	64	4	5	145	64

Hieraus folgt zugleich, dass wenn in einem Kettenbruche nach dem Subtraktionsprinzipe die Zeichen aller Quotienten von paaren Zeigern gleich und die Zeichen aller Quotienten von unpaaren Zeigern ebenfalls gleich, aber den ersteren entgegengesetzt sind, derselbe sich in einen Kettenbruch nach dem Additionsprinzipe mit lauter Quotienten von gleichen Zeichen verwandeln lässt, dass also nach §. 20, II die Näherungswerthe des ersteren auch den für den letzteren in §. 6 und 7 nachgewiesenen Gesetzen hinsichtlich der Fehlergränzen und der relativen Kleinheit der Zahlen Folge leisten.

§. 26. *Entwickelung eines gemeinen Bruches in einen Kettenbruch nach dem Subtraktionsprinzipe.*

I. Man schlägt hier ein dem früheren ganz gleiches Divisionsverfahren ein, ehe man jedoch mit einem verbliebenen Reste in den vorhergehenden Divisor dividirt, hat man das Zeichen jenes Restes in das entgegengesetzte zu verwandeln.

Im Übrigen kann man auch hier sowol Sub-, wie Superquotienten nehmen. Die bemerkenswerthesten Fälle sind folgende.

1) Zähler und Nenner des zu entwickelnden Bruches $\frac{M}{N}$ haben gleiche Zeichen, wie in $\frac{17}{5} = \frac{-17}{-5}$.

a) Alsdann sind die kleinsten Superquotienten sämmtlich positiv.

```
5|17|4
  20
 -3|5|2
   6
  -1|3|3
     3
     0
```

$\frac{17}{5} = [4, 2, 3]\ (-)$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	4	4	1
1	2	7	2
2	3	17	5

b) Von den grössten Subquotienten ist der erste a_0 positiv, alle übrigen negativ.

```
5|17|3
  15
 -2|5|-3
    6
   1|-2|-2
     -2
      0
```

$\frac{17}{5} = [3, -3, -2]\ (-)$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	3	3	1
1	-3	-10	-3
2	-2	17	5

c) Lässt man einen grössten Subquotienten $a_0, a_2, a_4 \ldots$ mit einem kleinsten Superquotienten $a_1, a_3, a_5 \ldots$ abwechseln; so werden die ersteren sämmtlich positiv und die letzteren negativ.

```
5|17|3
  15
 -2|5|-2
    4
  -1|-2|2
     -2
      0
```

$\frac{17}{3} = [3, 2, 2]\ (-)$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	3	3	1
1	-2	-7	-2
2	2	-17	-5

2) Zähler und Nenner des Bruches $\frac{M}{N}$ haben entgegengesetzte Zeichen, wie in $-\frac{17}{5} = \frac{-17}{5} = \frac{17}{-5}$.

a) Alsdann sind die grössten Subquotienten sämmtlich negativ.

```
5|-17|-4
  -20
  -3|5|-2
     6
    1|-3|-3
      -3
       0
```

$-\frac{17}{5} = [-4, -2, -3]\ (-)$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	-4	-4	1
1	-2	7	-2
2	-3	-17	5

b) Von den kleinsten Superquotienten ist der erste a_0 negativ, alle übrigen positiv.

$$\begin{array}{r|r|r} 5 & -17 & -3 \\ & -15 & \\ \hline & 2 & 5 \;|\; 3 \\ & & 6 \\ \hline & & 1 \;|\; 2 \;|\; 2 \\ & & 2 \\ \hline & & 0 \end{array} \qquad -\frac{17}{5} = [-3, 3, 2](-)$$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	-3	-3	1
1	3	-10	3
2	2	-17	5

c) Lässt man einen kleinsten Superquotienten a_0, a_2, a_4 . . . mit einem grössten Subquotienten a_1, a_3, a_5 . . . abwechseln; so werden die ersteren sämmtlich negativ und die letzteren positiv.

$$\begin{array}{r|r|r} 5 & -17 & -3 \\ & -15 & \\ \hline & 2 & 5 \;|\; 2 \\ & & 4 \\ \hline & & -1 \;|\; 2 \;|\; -2 \\ & & 2 \\ \hline & & 0 \end{array} \qquad -\frac{17}{5} = [-3, 2, -2](-)$$

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	-3	-3	1
1	2	-7	2
2	-2	17	-5

II. Will man Gelegenheit haben, auf die Entwickelung nach dem Subtraktionsprinzipe auch die Gesetze hinsichtlich der Fehlergränzen und der relativen Kleinheit der Zahlen in Anwendung zu bringen; so folgt aus Vorstehendem und aus §. 25, dass man bei einem positiven Bruche für a_0, a_2, a_4 . . . die grössten Subquotienten und für a_1, a_3, a_5 . . . die kleinsten Superquotienten, dass man dagegen bei einem negativen Bruche für a_0, a_2, a_4 . . . die kleinsten Superquotienten und für a_1, a_3, a_5 . . . die grösssten Subquotienten nehmen müsse. Die Entwickelung in diesen beiden Fällen wird stets eine endliche sein. Dies erhellet nicht bloss daraus, dass eine Umkehrung der Zeichen resp. der Quotienten von unpaaren oder von paaren Zeigern dieselben Quotienten erzeugt, welche man nach dem Additionsprinzipe resp. bei grössten Subquotienten oder kleinsten Superquotienten erhalten würde, sondern auch daraus, dass jeder Rest, absolut genommen, immer kleiner ist, als der vorhergehende Divisor.

Es ist aber hier, wie in §. 21 für die Entwickelung nach dem Additionsprinzipe, von besonderer, ja von noch grösserer Wichtigkeit, dass in den eben genannten beiden Fällen, welche sonst eine ganz besondere Aufmerksamkeit während der Rechnung erfordern würden, die sich ergebenden Quotienten stets die numerisch grössten Subquotienten sind.

Man wird also, zur Erreichung des bezeichneten Zweckes, sowol bei dem Additions-, als auch bei dem Subtraktionsprinzipe, gleichviel ob man es mit positiven oder mit negativen Brüchen zu thun hat, stets die numerisch grössten Subquotienten auswerfen, dabei aber das Zeichen nach den Regeln der Division verändern, und überhaupt das eigentliche Wesen resp. des Additions- oder des Subtraktionsprinzipes im Auge behalten.

III. Es versteht sich von selbst, dass man auch bei dem Subtraktionsprinzipe die in §. 22 beschriebene Entwickelung mit numerisch kleinsten Resten zur Anwendung bringen und daraus die schon früher bezeichneten Vortheile erwarten kann.

IV. Auch hier gilt die Bemerkung, dass wenn Zähler und Nenner des letzten Näherungswerthes das entgegengesetzte Zeichen von Zähler und Nenner des entwickelten Bruches haben sollten, man die Zeichen der Zähler und Nenner aller Näherungsbrüche umkehren kann, um dadurch den reduzirten Kettenbruch mit dem gegebenen vollständig zu identifiziren, was bei manchen Rechnungen ein Erforderniss ist.

So hat man z. B. für $-\frac{17}{5} = [-3, 2, -2]\,(-)$

eben sowol:

n	a_n	M_n	N_n
-2		0	-1
-1		1	0
0	-3	-3	1
1	2	-7	2
2	-2	17	-5

als auch:

n	a_n	M_n	N_n
-2		0	1
-1		-1	0
0	-3	3	-1
1	2	7	-2
2	-2	-17	5

Zweiter Abschnitt.

Auflösung der unbestimmten Gleichungen vom ersten Grade in ganzen Zahlen.

---

§. 27. *Allgemeine Begriffe und Vorbereitungen.*

I. Wenn die Anzahl gegebener Gleichungen kleiner ist, als die Anzahl der darin vorkommenden unbekannten Grössen; so heissen die Gleichungen schlechthin unbestimmte. Verlangt man jedoch, dass die Unbekannten ganze oder überhaupt rationale Zahlen seien; so nennt man jene Gleichungen zur besseren Unterscheidung wol diophantische, nach Diophantus, welcher derartige Aufgaben zuerst gestellt hat. Indessen ist es jetzt fast allgemein üblich, sich auch im letzteren Falle der Bezeichnung »unbestimmte Gleichungen« zu bedienen und da, wo es zur Vermeidung von Missverständnissen nöthig ist, ausdrücklich zu bemerken, dass es sich um eine Auflösung in ganzen oder rationalen Zahlen handele. Die hierher gehörigen Lehren begreift man unter dem Namen der unbestimmten Analytik, auch wol der diophanteischen Analysis. Das Wesen der ganzen Zahl spielt hierbei eine Hauptrolle, und demzufolge wird dieser Gegenstand auch der allgemeinen Untersuchung über die Gesetze der ganzen Zahlen einverleibt, welche von Legendre den Namen Theorie der Zahlen erhalten hat.

Im gegenwärtigen Abschnitte haben wir es nur mit Gleichungen vom ersten Grade mit rationalen Koeffizienten zu thun. Verlangte man bloss Auflösungen in rationalen Zahlen; so würden die gewöhnlichen Auflösungsmethoden vollkommen ausreichen. Man brauchte, wenn m Gleichungen mit $m+n$ Unbekannten gegeben wären, nur für n Unbekannte beliebige rationale Werthe oder allgemeine Zeichen, welche derartige rationale Grössen vertreten sollen, zu substituiren und die Gleichungen für die übrigen m Unbekannten aufzulösen. Das Resultat muss nothwendig auch für diese letzteren m Unbe-

kannten rationale Werthe ergeben. Demnach lassen wir die Auflösung der unbestimmten Gleichungen vom ersten Grade in rationalen Zahlen ganz ausser Acht, und beschäftigen uns nur mit deren Auflösungen in ganzen Zahlen.

II. Zunächst nehmen wir an, es sei eine einzige Gleichung mit zwei Unbekannten, deren allgemeinste Form

$$ax + by = k$$

ist, gegeben. Wären die Koeffizienten a, b, k Brüche; so brauchte man die ganze Gleichung nur mit einem Generalnenner dieser Brüche zu multipliziren, um lauter ganze Koeffizienten zu erhalten. Wir setzen also gleich von vorn herein ganze Koeffizienten voraus. Dieselben können übrigens positiv oder negativ sein, wie denn auch im Allgemeinen für die Unbekannten x und y nur ganze, positive oder negative Werthe erwartet werden.

III. Hätten die drei Koeffizienten a, b, k ein gemeinschaftliches Maass; so könnte die ganze Gleichung damit dividirt werden. Wir nehmen also an, a, b, k haben kein gemeinschaftliches Maass.

Ehe man hiernach zur Auflösung schreitet, hat man zu untersuchen, ob die beiden Koeffizienten a und b der Unbekannten für sich allein ein gemeinschaftliches Maass (ausser 1 oder — 1) besitzen. Ereignete sich Dies; so wäre die Auflösung in ganzen Zahlen unmöglich: denn es liesse sich alsdann für alle ganzen Werthe von x und y stets die linke Seite der gegebenen Gleichung durch das gemeinschaftliche Maass von a und b ohne Rest theilen, nicht aber die rechte. Es wird bemerkt, dass nur unter den letzteren Umständen die verlangte Auflösung unmöglich ist, dass dieselbe aber, wie aus Nachstehendem erhellet, stets möglich ist, wenn a und b relative Primzahlen sind.

§. 28. *Auflösung Einer Gleichung mit zwei Unbekannten durch Absonderung der grössten Ganzen.*

I. Nach Euler kann man die Auflösung der Gleichung

(1) $$ax + by = k$$

in ganzen Zahlen folgendermaassen bewirken. Man schafft die mit dem (absolut) grösseren Koeffizienten behaftete Unbekannte auf die rechte Seite und dividirt durch den kleineren Koeffizienten, lös't also in allgemeiner Form die gegebene Gleichung zuvörderst für diejenige Unbekannte auf, welche mit dem absolut kleineren Koeffizienten behaftet ist. Wenn also dem absoluten Werthe nach $b < a$; so lös't man für y auf und setzt

$$y = \frac{k - ax}{b} = \frac{k}{b} - \frac{a}{b}x$$

Jetzt sondert man aus den absoluten Werthen der Brüche $\frac{k}{b}$ und $\frac{a}{b}$ die grössten Ganzen ab, und schreibt demnach, wenn

$$\frac{k}{b} = m + \frac{r}{b}, \qquad \frac{a}{b} = n + \frac{s}{b}$$

also der absolute Werth von r und $s < b$ ist,

$$y = m - nx + \frac{r - s\,x}{b} = m - nx + w_1$$

Jetzt liegt, indem man $\frac{r - s\,x}{b} = w_1$ setzt, der Schluss nahe, dass wenn x und y ganze Zahlen sein sollen, nothwendig auch w_1 eine solche sein muss, und umgekehrt, dass wenn x und w_1 ganze Zahlen sind, auch y eine solche sein wird. Wir haben also die Gleichung

$$(2) \qquad \frac{r - s\,x}{b} = w_1$$

mit den beiden Unbekannten x und w_1 in ganzen Zahlen aufzulösen.

Zu diesem Ende multiplizirt man mit b und lös't, da $s < b$ ist, für x auf; dies gibt erst $r - s\,x = b\,w_1$ und dann

$$x = \frac{r - b\,w_1}{s} = \frac{r}{s} - \frac{b}{s}\,w_1$$

Hierauf sondert man wie vorhin aus den Brüchen $\frac{r}{s}$ und $\frac{b}{s}$ die grössten Ganzen ab, was, wenn $\frac{r}{s} = m_1 + \frac{r_1}{s}$, $\frac{b}{s} = n_1 + \frac{s_1}{s}$, also r_1 und $s_1 < s$ ist,

$$x = m_1 - n_1\,w_1 + \frac{r_1 - s_1 w_1}{s} = m_1 - n_1\,w_1 + w_2$$

ergibt. Jetzt wiederholt sich der frühere Schluss, dass wenn x und w_1 ganze Zahlen sein sollen, auch $\frac{r_1 - s_1 w_1}{s} = w_2$ eine solche sein muss, und umgekehrt, dass wenn w_1 und w_2 ganze Zahlen sind, auch x eine solche sein wird. Demnach hat man die neue Gleichung

$$(3) \qquad \frac{r_1 - s_1 w_1}{s} = w_2 \text{ oder } r_1 - s_1\,w_1 = s\,w_2$$

für die beiden Unbekannten w_1 und w_2 in ganzen Zahlen aufzulösen.

Zu diesem Ende lös't man, da $s_1 < s$ ist, für w_1, nämlich immer für die ältere Unbekannte auf und wiederholt die obige Operation. Das gibt jetzt die Ausdrücke

$$w_1 = \frac{r_1 - s w_2}{s_1} = \frac{r_1}{s_1} - \frac{s}{s_1} w_2 = m_2 - n_2 w_2 + \frac{r_2 - s_2 w_2}{s_1}$$
$$= m_2 - n_2 w_2 + w_3$$

(4) $$\frac{r_2 - s_2 w_2}{s_1} = w_3 \text{ oder } r_2 - s_2 w_2 = s_1 w_3$$

worin r_2 und $s_2 < s_1$ ist, ferner die Ausdrücke

$$w_2 = \frac{r_2 - s_1 w_3}{s_2} = \frac{r_2}{s_2} - \frac{s_1}{s_2} w_3 = m_3 - n_3 w_3 + \frac{r_3 - s_3 w_3}{s_2}$$
$$= m_3 - n_3 w_3 + w_4$$

(5) $$\frac{r_3 - s_3 w_3}{s_2} = w_4 \text{ oder } r_3 - s_3 w_3 = s_2 w_4 \text{ also}$$

(6) $$w_3 = \frac{r_3 - s_2 w_4}{s_3}$$

worin r_3 und $s_3 < s_2$ ist, u. s. w.

II. Da nun die absoluten Werthe der Zahlen a, b, s, s_1, s_2, s_3 . . . . eine abnehmende Reihe bilden, und a und b kein gemeinschaftliches Maass besitzen; so muss eine Fortsetzung des vorstehenden Verfahrens endlich auf eine Formel führen, welche wie die Gl. (6) gebildet ist, worin aber der absolute Werth des Nenners $= 1$, also $s_3 = \pm 1$, mithin

(7) $$w_3 = \pm (r_3 - s_2 w_4)$$

ist.

Diese Formel wird für jeden beliebigen ganzen Werth, den man anstatt w_4 darin setzen möge, erfüllt, und aus dem Obigen ist zugleich klar, dass auch nur ganze Werthe für w_4 gesetzt werden dürfen.

Man behält also w_4 als willkürliche Grösse, welcher alle ganze Werthe der unendlichen Reihe . . . $-2, -1, 0, 1, 2$ . . . beigelegt werden können, in der Auflösung bei, und substituirt nun, indem man die rückwärts laufende Reihe der Gleichungen

(8) $$\begin{cases} w_3 = \pm (r_3 - s_2 w_4) \\ w_2 = m_3 - n_3 w_3 + w_4 \\ w_1 = m_2 - n_2 w_2 + w_3 \\ x = m_1 - n_1 w_1 + w_2 \\ y = m - n x + w_1 \end{cases}$$

vor Augen nimmt, die Werthe der Grössen w mit späteren Zeigern in die Werthe dieser Grössen mit früheren Zeigern und zuletzt in die Werthe von x und y. Die hierdurch für x und y sich ergebenden Ausdrücke enthalten alsdann die Willkürliche w_4, welche wir kürzer mit w bezeichnen wollen, und stellen in der Form

(9) $$x = p + q w \qquad y = p_1 + q_1 w$$

wovon p, q, p_1, q_1 aus lauter bekannten Zahlen zusammengesetzt sind, die allgemeine Auflösung der gegebenen Gleichung dar.

III. Aus dem Vorstehenden erhellet, dass es andere Auflösungen, als solche, welche sich für $w = \ldots -3, -2, -1, 0, 1, 2, 3 \ldots$ herausstellen, nicht geben kann.

Wenn man aber erst eine einzige spezielle Auflösung für x und y berechnet hat, was am einfachsten immer für $w = 0$ geschieht, indem man hierfür $x = p$, $y = p_1$ hat; so ergeben sich daraus leicht alle übrigen, indem man zu einem früheren Werthe von x immer die Zahl q und zu dem korrespondirenden Werthe von y die Zahl q_1 entweder addirt oder subtrahirt. Denn es ist klar, dass wenn sich w um ± 1 ändert, x sich um $\pm q$ und y sich um $\pm q_1$ ändern muss.

IV. Im Laufe der obigen Rechnung kann es sich ereignen, dass Eine der mit r bezeichneten Grössen und damit alle folgenden verschwinden oder $= 0$ werden. Dieser Umstand ändert an dem beschriebenen Verfahren Nichts.

Es könnte sogar gleich von vorn herein das bekannte Glied in der gegebenen Gleichung fehlen oder $k = 0$ sein, indem man dann

(10) $$ax + by = 0$$

hätte. Auch dann verfährt man genau nach der gegebenen Regel. Man bemerkt jedoch leicht, dass in diesem Falle die gesuchte Auflösung sofort

(11) $$x = bw \qquad y = -aw$$

ist.

V. Hätten die beiden Koeffizienten a und b einen gleichen absoluten Werth, welcher, da beide relativ prim sein müssen, nur $= 1$ sein könnte, oder hätte auch nur ein einziger dieser beiden Koeffizienten den absoluten Werth 1, sodass also die gegebene Gleichung

(12) $$ax + y = k$$

wäre; so würde man für die mit dem Koeffizienten 1 behaftete Unbekannte den Werth $y = k - ax$ erhalten, worin die andere Unbekannte x sofort die Stelle der obigen Willkürlichen w verträte, sodass die gesuchte Auflösung

(13) $$x = w \qquad y = k - aw$$

wäre.

VI. In dem unmöglichen Falle, wo a und b ein gemeinschaftliches Maass haben, würden, wenn man die obige Rechnung in Anwendung bringen wollte, die Nenner der beiden Unbekannten, von welchen die Gleichung eben abhängig ist, eher verschwinden, als der Nenner des bekannten Gliedes, und Dies würde die unmögliche Forderung enthalten, dass ein Bruch (dessen Nenner nicht $= 1$ ist) gleich einer ganzen Zahl sei.

§. 20. Beispiele.

Beispiel 1. Es sei gegeben

$$25x + 13y = 37$$

Alsdann hat man

$$y = \frac{37 - 25x}{13} = 2 - x + \frac{11 - 12x}{13} = 2 - x + w_1$$

$$\frac{11 - 12x}{13} = w_1$$

$$x = \frac{11 - 13w_1}{12} = -w_1 + \frac{11 - w_1}{12} = -w_1 + w$$

$$\frac{11 - w_1}{12} = w$$

$$w_1 = 11 - 12w$$

folglich durch rückwärts gehende Substitution

$$x = -(11 - 12w) + w = -11 + 13w$$

$$y = 2 - (-11 + 13w) + (11 - 12w) = 24 - 25w$$

Dies gibt unter Anderem folgende spezielle Auflösungen

für $w = \ldots$	-3	-2	-1	0	1	2	3	...
$x = \ldots$	-50	-37	-24	-11	2	15	28	...
$y = \ldots$	99	74	49	24	-1	-26	-51	...

Nach rechts setzt sich die Reihe der x und y resp. durch Addition von 13 und -25, nach links dagegen resp. durch Subtraktion von 13 und -25 fort.

Beispiel 2. Es sei gegeben

$$23x - 15y = 30$$

Alsdann hat man

$$y = \frac{-30 + 23x}{15} = -2 + x + \frac{8x}{15} = -2 + x + w_1$$

$$\frac{8x}{15} = w_1$$

$$x = \frac{15w_1}{8} = w_1 + \frac{7w_1}{8} = w_1 + w_2$$

$$\frac{7w_1}{8} = w_2$$

$$w_1 = \frac{8w_2}{7} = w_2 + \frac{w_2}{7} = w_2 + w$$

$$\frac{w_2}{7} = w$$

$$w_2 = 7w$$

folglich durch rückwärts gehende Substitution

$$w_1 = 7w + w = 8w$$

$$x = 8w + 7w = 15w$$

$$y = -2 + 15w + 8w = -2 + 23w$$

Dies gibt unter Anderem folgende spezielle Auflösungen

für $w = \ldots$	-3	-2	-1	0	1	2	$3 \ldots$
$x = \ldots$	-45	-30	-15	0	15	30	$45 \ldots$
$y = \ldots$	-71	-48	-25	-2	21	44	$67 \ldots$

Nach rechts setzt sich die Reihe der x und y resp. durch Addition von 15 und 23, nach links dagegen resp. durch Subtraktion von 15 und 23 fort.

Beispiel 3. Es sei gegeben

$$13x - 17y = 0$$

Hier hat man sofort

$$x = 17w \qquad y = 13w$$

also als spezielle Auflösungen

für $w = \ldots$	-3	-2	-1	0	1	2	$3 \ldots$
$x = \ldots$	-51	-34	-17	0	17	34	$51 \ldots$
$y = \ldots$	-39	-26	-13	0	13	26	$39 \ldots$

Beispiel 4. Es sei gegeben

$$10x - y = -7$$

Alsdann ist

$$x = w \qquad y = 7 + 10w$$

also als spezielle Auflösungen

für $w = \ldots$	-3	-2	-1	0	1	2	$3 \ldots$
$x = \ldots$	-3	-2	-1	0	1	2	$3 \ldots$
$y = \ldots$	-23	-13	-3	7	17	27	$37 \ldots$

Beispiel 5. Es sei die unmögliche Gleichung

$$4x + 6y = 5$$

gegeben. Die obige Methode ergibt folgende Rechnung

$$x = \frac{5 - 6y}{4} = 1 - y + \frac{1 - 2y}{4} = 1 - y + w_1$$

$$\frac{1 - 2y}{4} = w_1$$

$$y = \frac{1 - 4w_1}{2} = -2w_1 + \frac{1}{2} = -2w_1 + w$$

$$\frac{1}{2} = w$$

Dies führt also zu der ungereimten Forderung, dass der Bruch $\frac{1}{2}$ gleich einer ganzen Zahl w sei.

§. 30. *Auflösung der Gleichung ax — by = 1 mit Hülfe der Kettenbrüche nach dem Additionsprincipe.*

I. Lagrange hat hervorgehoben, was bis dahin unbeachtet geblieben zu sein scheint, dass Bachet von Meziriac der Erste gewesen sei, welcher die Kettenbrüche zur Auflösung der unbestimmten Gleichungen vom ersten Grade verwendet habe. Wir werden hier die Entwickelungen sogleich unter einem allgemeineren Gesichtspunkte durchführen, als Dies gewöhnlich geschieht.

Wenn in der Gleichung

(1) $$ax - by = 1$$

a und b zwei positive oder negative, aber relativ prime Zahlen sind; so ist dieselbe in ganzen Zahlen stets auflösbar. Denn entwickelt man den auf seiner kleinsten Benennung erscheinenden Bruch $\frac{a}{b}$ in einen Kettenbruch nach dem Additionsprinzipe, bezeichnet den Zeiger des letzten Quotienten mit n, setzt also nach der Bezeichnungsweise des ersten Abschnittes

(2) $$M_n = a \qquad N_n = b \qquad \frac{M_n}{N_n} = \frac{a}{b}$$

so hat man nach §. 4, wenn M_{n-1}, N_{n-1} Zähler und Nenner des vorletzten Näherungsbruches sind,

$$M_n\, N_{n-1} - N_n\, M_{n-1} = (-1)^{n-1}$$

oder auch

$$M_n\,.\,(-1)^{n-1}\, N_{n-1} - N_n\,.\,(-1)^{n-1}\, M_{n-1} = 1 \text{ oder}$$
$$a\,.\,(-1)^{n-1}\, N_{n-1} - b\,.\,(-1)^{n-1}\, M_{n-1} = 1$$

Vergleicht man diese Gleichung mit der gegebenen; so ergibt sich die spezielle Auflösung

(3) $$x = (-1)^{n-1}\, N_{n-1} \qquad y = (-1)^{n-1}\, M_{n-1}$$

Die hier verlangte Kettenbruchsentwickelung von $\frac{a}{b}$ braucht nur nach dem Additionsprinzipe durchgeführt zu sein, kann aber beliebige willkürliche Quotienten enthalten. Es ist jedoch wichtig, zu bemerken, dass man für x und y die Auflösung in den kleinstmöglichen Zahlen erhält, wenn man den Kettenbruch mit numerisch grössten Subquotienten entwickelt (§. 21).

In allen Fällen ist übrigens dafür zu sorgen, dass der Zähler und Nenner des letzten Näherungswerthes $\frac{M_n}{N_n}$ die Zahlen a und b auch hinsichtlich des ihnen zukommenden Zeichens vollständig wiedergebe (§. 21, II).

Wenn man nach §. 22 mit numerisch kleinsten Resten entwickelt, hat man im Allgemeinen die kürzeste Rechnung zu erwarten.

Beispiel 1. $50\,x - 23\,y = 1$

Man hat hier mit numerisch grössten Subquotienten

$$\frac{50}{23} = [2,\ 5,\ 1,\ 3]$$

n	a_n	M_n	N_n
−2		0	1
−1		1	0
0	2	2	1
1	5	11	5
2	1	13	6
3	3	50	23

$n = 3$, $n - 1 = 2$, $(-1)^{n-1} = (-1)^2 = 1$

$M_{n-1} = M_2 = 13$, $N_{n-1} = N_2 = 6$

$x = (-1)^{n-1} N_{n-1} = 6$ $y = (-1)^{n-1} M_{n-1} = 13$

Beispiel 2. $-8x + 25y = (-8)x - (-25)y = 1$

Man hat hier mit numerisch grössten Subquotienten

$\frac{-8}{-25} = [0, 3, 7, 1]$

n	a_n	M_n	N_n
-2		0	-1
-1		-1	0
0	0	0	-1
1	3	-1	-3
2	7	-7	-22
3	1	-8	-25

$x = (-1)^{n-1} N_{n-1} = (-1)^2 N_2 = -22$

$y = (-1)^{n-1} M_{n-1} = (-1)^2 M_2 = -7$

Beispiel 3. $17x + 3y = 17x - (-3)y = 1$

Man hat hier mit numerisch grössten Subquotienten

$\frac{17}{-3} = [-5, -1, -2]$

n	a_n	M_n	N_n
-2		0	-1
-1		-1	0
0	-5	5	-1
1	-1	-6	1
2	-2	17	-3

$x = (-1)^{n-1} N_{n-1} = (-1)^1 N_1 = -1$

$y = (-1)^{n-1} M_{n-1} = (-1)^1 M_1 = 6$

Beispiel 4. $-17x - 3y = (-17)x - 3y = 1$

Man hat hier mit numerisch grössten Subquotienten

$\frac{-17}{3} = [-5, -1, -2]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	-5	-5	1
1	-1	6	-1
2	-2	-17	3

$x = (-1)^{n-1} N_{n-1} = (-1)^1 N_1 = 1$

$y = (-1)^{n-1} M_{n-1} = (-1)^1 M_1 = -6$

II. Die Unbestimmtheit der gegebenen Gleichung macht sich daran kenntlich, dass es statthaft ist, bei der Entwickelung von $\frac{M_n}{N_n} = \frac{a}{b}$ in einen Kettenbruch willkürliche Quotienten einzuführen. Es würde jedoch sehr umständlich sein, durch Veränderung dieser willkürlichen Quotienten nach und nach verschiedene Auflösungen zu erzielen. In §. 32 wird man sehen, dass es nur der Kenntniss einer einzigen speziellen Auflösung bedarf, um eine Formel aufzustellen, welche alle möglichen Auflösungen der gegebenen Gleichung darstellt.

Will man übrigens das Prinzip der Kettenbrüche zur Hervorbringung dieser verschiedenen Auflösungen verwenden; so ist es rathsam, das obige Verfahren folgendermaassen zu modifiziren.

Wir gehen, indem wir auch jetzt $M_n = a$, $N_n = b$ setzen und $\frac{M_n}{N_n} = \frac{a}{b}$ in einen Kettenbruch entwickeln, von der Formel

$$M_n N_{n+1} - N_n M_{n+1} = (-1)^{n+1} \text{ oder}$$
$$M_n . (-1)^{n+1} N_{n+1} - N_n . (-1)^{n+1} M_{n+1} = 1 \text{ oder}$$
$$a . (-1)^{n+1} N_{n+1} - b . (-1)^{n+1} M_{n+1} = 1$$

aus, welche uns die Auflösung

(4) $$x = (-1)^{n+1} N_{n+1}, \qquad y = (-1)^{n+1} M_{n+1}$$

liefert.

In diesen Formeln bezeichnet n den Zeiger des letzten Quotienten des in einen Kettenbruch verwandelten Bruches $\frac{a}{b}$, sodass man also $\frac{a}{b} = [a_0, a_1 \ldots a_n]$ hat. Um die Auflösungen für x und y zu erhalten, welche die Fortsetzung dieses Kettenbruches um Ein Glied, nämlich bis zum Zeiger $n+1$ verlangen, kann man auf den letzten Quotienten a_n als nächsten Quotienten a_{n+1} j e d e b e l i e b i g e g a n z e Z a h l w (welche auch 0 und negativ sein kann) folgen lassen.

So hat man in dem obigen Beispiele 1, jenachdem man auf den letzten Quotienten der Entwickelung von $\frac{50}{23}$ die Zahl -1 oder 0 oder 1 oder 2 etc. folgen lässt, resp. den nachstehenden Schluss der Rechnung

n	a_n	M_n	N_n	a_n	M_n	N_n	a_n	M_n	N_n	a_n	M_n	N_n
2		13	6		13	6		13	6		13	6
3		50	23		50	23		50	23		50	23
4	-1	-37	-17	0	13	6	1	63	29	2	113	52

also resp.

$$x = (-1)^{n+1} N_{n+1} = N_4 = -17 \quad 6 \quad 29 \quad 52$$
$$y = (-1)^{n+1} M_{n+1} = M_4 = -37 \quad 13 \quad 63 \quad 113$$

§. 31. *Auflösung der Gleichung* $ax - by = 1$ *mit Hülfe der Kettenbrüche nach dem Subtraktionsprinzipe.*

Die nach dem Subtraktionsprinzipe gebildeten Kettenbrüche ergeben ein in mancher Beziehung noch einfacheres, wenigstens bemerkenswerthes Mittel zur Auflösung der vorstehenden Gleichung an die Hand. Um hiernach die Gleichung

(1) $$ax - by = 1$$

zu lösen, gehen wir von der Beziehung §. 24

$$N_n M_{n-1} - M_n N_{n-1} = 1$$

aus, nehmen also

(2) $$M_n = b \qquad N_n = a \qquad \frac{M_n}{N_n} = \frac{b}{a}$$

und entwickeln den Bruch $\frac{b}{a}$ nach dem Subtraktionsprinzipe in einen Kettenbruch. Der vorletzte Näherungsbruch $\frac{M_{n-1}}{N_{n-1}}$ liefert

alsdann sofort die Auflösung

(3) $x = M_{n-1} \qquad y = N_{n-1}$

Auch hier können in die Entwickelung willkürliche Quotienten eintreten. Will man jedoch die Auflösung in den kleinstmöglichen Zahlen haben; so muss man die Entwickelung mit numerisch grössten Subquotienten machen (§. 26, II.)

Übrigens darf auch hier niemals versäumt werden, dafür zu sorgen, dass im Zähler und Nenner des letzten Näherungsbruches $\frac{M_n}{N_n}$ die Zahlen b und a nach ihrem Zeichen vollständig wiedererscheinen (§. 26, IV.)

Beispiel 1. $5x - 17y = 1$

Man hat hier mit numerisch grössten Subquotienten

$$\frac{17}{5} = [3, -2, 2] \ (-)$$

n	a_n	M_n	N_n
-2		0	1
-1		-1	0
0	3	-3	-1
1	-2	7	2
2	2	17	5

$$x = M_{n-1} = M_1 = 7$$
$$y = N_{n-1} = N_1 = 2$$

Beispiel 2. $5x + 17y = 5x - (-17)y = 1$

Man hat hier mit numerisch grössten Subquotienten

$$\frac{-17}{5} = [-3, 2, -2] \ (-)$$

n	a_n	M_n	N_n
-2		0	1
-1		-1	0
0	-3	3	-1
1	2	7	-2
2	-2	-17	5

$$x = M_{n-1} = M_1 = 7$$
$$y = N_{n-1} = N_1 = -2$$

Schliesslich wird noch bemerkt, dass auch die Kettenbrüche nach dem Subtraktionsprinzipe die Anwendung der im vorhergehenden Paragraphen sub II. gelehrten Methode behuf Bestimmung der unendlich vielen Auflösungen gestatten, wenn man hier von der Formel $M_n N_{n+1} - N_n M_{n+1} = 1$ ausgeht, also $M_n = a$, $N_n = b$ setzt, $\frac{M_n}{N_n} = \frac{a}{b}$ in einen Kettenbruch nach dem Subtraktionsprinzipe verwandelt und dann unter Hinzufügung eines willkürlichen Quotienten

$$x = N_{n+1} \qquad y = M_{n+1}$$

nimmt.

§. 32. *Auflösung der Gleichung* ax — by = k *mit Hülfe der Kettenbrüche.*

Wenn durch §. 30 oder 31 $x = u$, $y = v$ als eine spezielle Auflösung der Gleichung $ax - by = 1$ gefunden ist; so ist offenbar $x = ku$, $y = kv$ eine spezielle Auflösung der Gleichung

(1) $ax - by = k$

Die allgemeine Auflösung dieser Gleichung ist aber, wenn w irgend eine willkürliche ganze Zahl bezeichnet,

(2) $$x = ku + bw \qquad y = kv + aw$$

und diese Formeln gelten auch dann für die allgemeine Auflösung der gegebenen Gleichung, selbst wenn darin $k = 1$ sein sollte.

Dass die letzteren Ausdrücke der gegebenen Gleichung wirklich genügen, leuchtet ein, dass sie aber auch alle möglichen Auflösungen enthalten, geht aus Folgendem hervor.

Es seien x_1, y_1 und x_2, y_2 zwei spezielle Auflösungen der gegebenen Gleichung, also

$$ax_1 - by_1 = k$$

$$ax_2 - by_2 = k \text{ und demnach}$$

$$a(x_2 - x_1) = b(y_2 - y_1) \text{ oder}$$

$$x_2 - x_1 = b\left(\frac{y_2 - y_1}{a}\right) \qquad y_2 - y_1 = a\left(\frac{x_2 - x_1}{b}\right) \text{ und auch}$$

$$x_2 = x_1 + b\left(\frac{y_2 - y_1}{a}\right) \qquad y_2 = y_1 + a\left(\frac{x_2 - x_1}{b}\right)$$

Da a und b relativ prim sind; so ist klar, dass in den Brüchen $b\left(\frac{y_2 - y_1}{a}\right)$ und $a\left(\frac{x_2 - x_1}{b}\right)$, welche durchaus ganze Zahlen sein müssen, a in $y_2 - y_1$ und b in $x_2 - x_1$ aufgehen muss. Alsdann erkennt man aber, dass die zweite Auflösung x_2, y_2 stets der obigen Form, welche als die allgemeine bezeichnet ist, entspricht.

Aus Vorstehendem erkennt man, dass die Bekanntschaft irgend einer speziellen Auflösung x_1, y_1 der gegebenen Gleichung genügt, um sofort die allgemeine Auflösung

(3) $$x = x_1 + bw \qquad y = y_1 + aw$$

zu bilden, worin w jede ganze Zahl vertritt.

In diesen Formeln kann man unbeschadet ihrer Allgemeinheit, wenn m eine beliebige konstante Zahl bezeichnet, $w = m \pm w'$ also

$$x = (x_1 + bm) \pm bw' \qquad y = (y_1 + am) \pm aw'$$

setzen, worin nun w' die Willkürliche ist.

Setzte man jedoch $w = mw'$; so würden zwar die Ausdrücke

$$x = x_1 + bm\,w' \qquad y = y_1 + am\,w'$$

für jeden ganzen Werth von w' eine Auflösung der gegebenen Gleichung liefern: allein diese Ausdrücke stellen nicht die allgemeine Auflösung dar. Denn bei der Variation der Willkürlichen w' um je Eine Einheit längs der Reihe aller ganzen Zahlen ... -2, -1, 0, 1, 2 ... wächst x immer um bm und y um am; es werden also immer $m-1$ Auflösungen übersprungen.

Aus Obigem kann man noch die Bemerkung ziehen, dass unter den Auflösungen der Gleichung $ay - by = k$ stets eine

unendliche Menge solcher enthalten sind, welche die Grösse k als **gemeinschaftliches Maass** besitzen. Unter anderen gehört hierzu die Auflösung $x = ku$, $y = kv$.

Wenn $k = 0$, also die Gleichung $ax - by = 0$ gegeben ist; so würde man die Kettenbruchsentwickelung ganz unterlassen können, da man stets $ku = 0$, $kv = 0$, also als allgemeine Auflösung $x = bw$, $y = aw$ hat.

Ebenso erweis't sich diese Entwickelung für den schon in §. 28 erwähnten Fall, wo a oder $b = \pm 1$ ist, als überflüssig.

In jedem andern Falle bewirkt man die Auflösung der Gleichung

$$ax - by = k$$

entweder nach folgender Regel: man entwickelt $\frac{a}{b} = \frac{M_n}{N_n}$ nach dem **Additionsprinzipe** in einen Kettenbruch (bei welchem M_n, N_n auch dem **Zeichen** nach resp. $= a$, b werden müssen) und setzt

(4) $x = (-1)^{n-1}\, kN_{n-1} + bw \qquad y = (-1)^{n-1}\, kM_{n-1} + aw$

oder nach folgender Regel: man entwickelt $\frac{b}{a} = \frac{M_n}{N_n}$ nach dem **Subtraktionsprinzipe** in einen Kettenbruch (bei welchem M_n, N_n auch dem **Zeichen** nach resp. $= b$, a werden müssen) und setzt

(5) $x = kM_{n-1} + bw \qquad y = kN_{n-1} + aw$

§. 33. *Beispiele.*

Beispiel 1. Mit wie viel Louisd'oren zu $5\frac{1}{2}$ Thlr. und Gulden zu $\frac{2}{3}$ Thlr. kann man eine Summe von 100 Thlr. bezahlen?

Bezeichnet man die Anzahl der Louisd'ore mit x und die der Gulden mit y; so muss man haben

$$5\tfrac{1}{2}\, x + \tfrac{2}{3}\, y = 100 \text{ oder}$$
$$33\, x + 4\, y = 33\, x - (-4)\, y = 600$$

Entwickelt man $\frac{33}{-4}$ nach dem Additionsprinzipe in einen Kettenbruch; so kommt $[-8, -4]$, also

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	-8	-8	1
1	-4	33	-4

$u = (-1)^{n-1}\, N_{n-1} = (-1)^0\, N^0 = 1$

$v = (-1)^{n-1}\, M_{n-1} = (-1)^0\, M_0 = -8$

$$x = 600 \,.\, 1 + (-4)w = 600 - 4w$$
$$y = 600 \,.\, (-8) + 33w = -4800 + 33w$$

Da hier offenbar negative Werthe für x oder y auszuschliessen sind; so reduzirt sich die unendliche Menge aller möglichen Auflösungcn auf die folgenden fünf

für z =	146	147	148	149	150	
x =	16	12	8	4	0	Louisd'ore
y =	18	51	84	117	150	Gulden

Beispiel 2. Welche Anzahl lässt, nach Dutzenden gezählt 7 Stück und nach Mandeln gezählt, 1 Stück übrig?

Die fragliche Anzahl z muss offenbar sowol der Form $12\,x + 7$, wie auch der Form $15\,y + 1$ entsprechen. Man hat also

$$12\,x + 7 = 15\,y + 1 \text{ oder}$$

$$12\,x - 15\,y = -6 \text{ und wenn man mit 3 dividirt,}$$

$$4\,x - 5\,y = -2$$

Entwickelt man $\frac{4}{5}$ nach dem Additionsprinzipe in einen Kettenbruch; so kommt [0, 1, 4], also

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	4	4	5

$$u = (-1)^{n-1}\,N_{n-1} = (-1)^1\,N_1 = -1$$

$$v = (-1)^{n-1}\,M_{n-1} = (-1)^1\,M_1 = -1$$

$$x = -2\,(-1) + 5\,w = 2 + 5\,w$$

$$y = -2\,(-1) + 4\,w = 2 + 4\,w$$

Die gesuchte Anzahl ist also

$$z = 12\,x + 7 = 15\,y + 1 = 31 + 60\,w$$

Man wird hier für z nur positive Werthe zulassen wollen. Die gesuchten Auflösungen sind also

für w =	0	1	2	3	...
z =	31	91	151	211	...

§. 33a. *Anwendung auf die Zerlegung und Decimalentwickelung gewöhnlicher Brüche.*

I. Wenn $\frac{p}{q}$ irgend einen gewöhnlichen positiven oder negativen Bruch darstellt, dessen Zähler p jeden beliebigen positiven oder negativen Werth haben kann, dessen positiver Nenner q aber das Produkt irgend zweier relativ primer Zahlen a, b ist; so lässt sich jener Bruch immer als die Summe oder Differenz zweier anderen Brüche $\frac{x}{a}$, $\frac{y}{b}$ darstellen, deren Nenner gleich den Faktoren a, b des Nenners q sind.

Denn damit für ganze Werthe von x und y die Gleichung

$$(1) \qquad \frac{x}{a} + \frac{y}{b} = \frac{p}{q} = \frac{p}{ab}$$

bestehe, muss die unbestimmte Gleichung

$$(2) \qquad bx + ay = p$$

in ganzen Zahlen lösbar sein, was unter der gemachten Voraussetzung, wonach a und b relativ prim sind, stets möglich ist.

So hat man z. B. für den Bruch $\frac{p}{q} = \frac{152}{315}$, wenn man dessen Nenner $315 = 5 \cdot 63 = a \cdot b$ setzt,

$$63x + 5y = 152$$

also $x = \quad 5w - 1 = \ldots \quad 9 \quad 4 \quad -1 \quad -6 \ldots$

$y = -63w + 43 = \ldots -79 \quad -20 \quad 43 \quad 106 \ldots$

Der Bruch $\frac{152}{315}$ kann also unter Anderem in folgender Weise zerlegt werden

$$\frac{152}{315} = \frac{9}{5} - \frac{79}{63} = \frac{4}{5} - \frac{20}{63} = -\frac{1}{5} + \frac{43}{63} = -\frac{6}{5} + \frac{106}{63} \text{ etc.}$$

Man erkennt, dass dieser Bruch $\frac{152}{315}$ nur als eine Differenz, nicht als eine Summe zweier positiven Brüche von den Nennern 5 und 63 dargestellt werden kann.

II. Es ist immer möglich, den Zähler x des ersten Bruches $\frac{x}{a}$, worin $\frac{p}{q}$ zerlegt ist, positiv und kleiner als a zu machen, sodass also der Bruch $\frac{x}{a}$ positiv und echt wird.

Dies leuchtet ein, wenn man erwägt, dass die allgemeine Auflösung der Gl. (2) in der Form

(3) $\qquad x = r - aw, \quad y = s + bw$

erscheint, worin w jede willkürliche positive oder negative ganze Zahl darstellt, welche leicht so genommen werden kann, dass x positiv und kleiner als a wird.

Da sich alle möglichen Werthe von x durch Vielfache der Grösse a von einander unterscheiden; so ist klar, dass es nur einen einzigen Werth von x geben kann, welcher der vorstehenden Bedingung gemäss positiv und kleiner als a ist.

Im obigen Beispiele hat man für diesen Fall die einzige Zerlegung

$$\frac{152}{315} = \frac{4}{5} - \frac{20}{63}$$

III. Wenn $a, b, c, d \ldots$ die Primzahlen oder die Potenzen von Primzahlen sind, in welche sich der Nenner q des Bruches $\frac{p}{q}$ zerlegen lässt, so dass man also $q = abcd \ldots n$ hat; so kann man den Bruch $\frac{p}{q}$ nach Vorstehendem zuvörderst in die beiden Brüche $\frac{x'}{a} + \frac{y'}{bcd \ldots n}$ zerlegen, worin der erste $\frac{x'}{a}$ positiv und echt ist. Hierauf kann man den zweiten Bruch $\frac{y'}{bcd \ldots n}$, gleichviel ob derselbe positiv oder negativ ist, in die beiden Brüche

$\frac{x''}{b}+\frac{y''}{cd\ldots n}$ zerlegen, worin wiederum der erste $\frac{x''}{b}$ positiv und echt ist. Alsdann kann man den Bruch $\frac{y''}{cd\ldots n}$ in die beiden Brüche $\frac{x'''}{c}+\frac{y'''}{d\ldots n}$ zerlegen, deren erster $\frac{x'''}{c}$ positiv und echt ist. Durch Fortsetzung dieser Operation zerfällt der gegebene Bruch $\frac{p}{q}$ in die Summe

$$(4)\qquad \frac{p}{q}=\frac{x'}{a}+\frac{x''}{b}+\frac{x'''}{c}+\ldots+\frac{y}{n}$$

worin alle Theile mit Ausnahme des letzten $\frac{y}{n}$ positiv und echt sind. Ergäbe sich aber durch das vorstehende Verfahren für den letzten Theil $\frac{y}{n}$ ein Werth, welcher nicht gleichzeitig positiv und echt wäre; so kann man, wenn k eine positive ganze Zahl bezeichnet, dieselbe immer so wählen, dass in

$$(5)\qquad \frac{y}{n}=\frac{x}{n}\mp k$$

der Bruch $\frac{x}{n}$ positiv und echt wird.

Demnach lässt sich der gegebene Bruch stets in die Form

$$(6)\qquad \frac{p}{abc\ldots n}=\mp k+\frac{x'}{a}+\frac{x''}{b}+\frac{x'''}{c}+\ldots+\frac{x}{n}$$

bringen, worin k eine ganze Zahl und jeder der folgenden Brüche positiv und echt ist.

So ist z. B. im obigen Beispiele $\frac{125}{315}=\frac{125}{5.7.9}$. Nachdem man die schon vorhin ermittelte erste Zerlegung $\frac{4}{5}-\frac{20}{7.9}$ vorgenommen hat, ist ferner der Bruch $-\frac{20}{7.9}$ in die Form $\frac{x}{7}+\frac{y}{9}$ zu zerlegen, also die Gleichung $9x+7y=-20$ zu lösen. Dies gibt $-\frac{20}{7.9}=\frac{4}{7}-\frac{8}{9}$.

Demnach ist

$$\frac{152}{315}=\frac{4}{5}+\frac{4}{7}-\frac{8}{9}$$
$$=-1+\frac{4}{5}+\frac{4}{7}+\frac{1}{9}$$

IV. In den *Disquisitiones arithmeticae, art.* 317 hat Gauss auf den praktischen Nutzen aufmerksam gemacht, welchen man bei der Entwickelung eines Bruches $\frac{p}{q}$ in einen Dezimalbruch

aus der vorstehenden Zerlegung in den Fällen ziehen kann, wo q eine sehr grosse Zahl ist, welche sich in bedeutend kleinere Primfaktoren $a, b, c \ldots$ oder Potenzen davon zerlegen lässt. Man braucht dann offenbar nur die einzelnen Brüche $\frac{x'}{a}, \frac{x''}{b}, \frac{x''}{c} \ldots$ in Dezimalbrüche zu verwandeln und die Summe nach (6) zu bilden.

So hat man z. B. für den Bruch

$$\frac{152}{315} = -1 + \frac{4}{5} + \frac{4}{7} + \frac{1}{9}$$

$$\frac{4}{5} = 0{,}8$$

$$\frac{4}{7} = 0{,}571\,428\,571\,428 \ldots$$

$$\frac{1}{9} = 0{,}111\,111\,111\,111 \ldots$$

$$\frac{152}{315} = 0{,}482\,539\,682\,539 \ldots$$

§. 34. *Auflösung Einer Gleichung mit drei Unbekannten für den Fall, wo zwei Koeffizienten relativ prim sind.*

Nachdem dafür gesorgt ist, dass in der Gleichung

(1) $$ax + by + cz = k$$

die vier Koeffizienten a, b, c, k ganze Zahlen ohne ein gemeinschaftliches Maass sind, dürfen, wenn die Auflösung möglich sein soll, die drei Koeffizienten a, b, c kein gemeinschaftliches Maass haben. Wenn aber a, b, c relativ prim sind; so ist die Auflösung stets möglich und wird folgendermaassen bewirkt.

Wir unterscheiden zwei Fälle, nämlich den, wo unter den drei Koeffizienten a, b, c zwei, z. B. a und b vorkommen, welche relativ prim sind, und ferner den, wo je zwei dieser Koeffizienten ein gemeinschaftliches Maass haben.

Im ersten Falle, wo also a und b relativ prim sind, lässt man die damit behafteten Unbekannten links stehen und transponirt das dritte Glied nach rechts. Dies giebt

(2) $$ax + by = k - cz$$

Indem man nun z wie eine bekannte, aber völlig willkürliche ganze Zahl behandelt, kann man die vorstehende Gleichung entweder nach der Methode des §. 28 auflösen, wobei man nach Belieben auch aus den mit z behafteten Gliedern die grössten Ganzen aussondern kann, oder auch nach der Methode des §. 32, wobei man dann schliesslich berücksichtigt, dass das bekannte Glied auf der rechten Seite der gegebenen Gleichung, welches früher mit k bezeichnet war, jetzt $k - cz$ ist.

Durch die Eine, wie durch die andere Auflösung wird man für x und y Ausdrücke erhalten, in welchen neben der ersten

Willkürlichen z noch eine andere von z ganz unabhängige Willkürliche w erscheint.

§. 35. *Beispiele.*

Beispiel 1. Wie viel Pferde zu 50 Thlr., Kühe zu 20 Thlr. und Schafe zu $3\frac{1}{2}$ Thlr. kann man für $328\frac{1}{2}$ Thlr. kaufen?

Es seien x Pferde, y Kühe, z Schafe; alsdann hat man $50x + 20y + 3\frac{1}{2}z = 328\frac{1}{2}$ oder nach Multiplication mit 2

$$100x + 40y + 7z = 657$$

Hier dürfen auf der linken Seite nicht die beiden Unbekannten x und y stehen bleiben, weil ihre Koeffizienten ein gemeinschaftliches Maass 20 haben. Wol aber können y und z links stehen bleiben. Dies gibt

$$40y + 7z = 657 - 100x$$

worin nun x die Eine Willkürliche ist.

Lös't man diese Gleichung für y und z nach §. 28 auf; so kommt

$$z = \frac{657 - 100x - 40y}{7} = 93 - 14x - 5y + \frac{6 - 2x - 5y}{7}$$
$$= 93 - 14x - 5y + w_1$$
$$\frac{6 - 2x - 5y}{7} = w_1$$
$$y = \frac{6 - 2x - 7w_1}{5} = 1 - w_1 + \frac{1 - 2x - 2w_1}{5} = 1 - w_1 + w_2$$
$$\frac{1 - 2x - 2w_1}{5} = w_2$$
$$w_1 = \frac{1 - 2x - 5w_2}{2} = -x - 2w_2 + \frac{1 - w_2}{2}$$
$$= -x - 2w_2 + w$$
$$\frac{1 - w_2}{2} = w$$
$$w_2 = 1 - 2w$$

Durch rückwärts gehende Substitution erhält man

$$w_1 = -x - 2(1 - 2w) + w = -2 - x + 5w$$
$$y = 1 - (-2 - x + 5w) + (1 - 2w) = 4 + x - 7w$$
$$z = 93 - 14x - 5(4 + x - 7w) + (-2 - x + 5w)$$
$$= 71 - 20x + 40w$$

Die Bildung der Werthe einer von zwei Willkürlichen w, w_1 in der Form $p + qw + rw_1$ abhängigen Grösse kann, wenn für ein gewisses w und w_1 ein einziger Werth berechnet ist, durch einfache Addition oder Subtraktion geschehen.

Ordnet man nämlich jene Werthe in einer Tabelle mit horizontalen und vertikalen Spalten, sodass die horizontalen Spalten den Variationen von w bei einem konstanten w_1 und

die vertikalen Spalten den Variationen von w_1 für ein konstantes w entsprechen; so braucht man nur zu beachten, dass wenn w um 1 wächst, die Werthe in den horizontalen Spalten um q wachsen, und wenn w_1 um 1 wächst, die Werthe in den vertikalen Spalten um r wachsen.

Dies gibt in dem obigen Beispiele in dem Zwischenraume von $x = 0$ bis $x = 5$ und von $w = -3$ bis $w = 3$ folgende Auflösungen

für $y = 4 + x - 7w$

w ‖ $x =$	0	1	2	3	4	5
-3	25	26	27	28	29	30
-2	18	19	20	21	22	23
-1	11	12	13	14	15	16
0	4	5	6	7	8	9
1	-3	-2	-1	0	1	2
2	-10	-9	-8	-7	-6	-5
3	-17	-16	-15	-14	-13	-12

für $z = 71 - 20x + 40w$

w ‖ $x =$	0	1	2	3	4	5
-3	-49	-69	-89	-109	-129	-149
-2	-9	-29	-49	-69	-89	-109
-1	31	11	-9	-29	-49	-69
0	71	51	31	11	-9	-29
1	111	91	71	51	31	11
2	151	131	111	91	71	51
3	191	171	151	131	111	91

Da nach der Natur der Aufgabe x, y, z positiv sein müssen; so hat man in dem genannten Zwischenraume folgende brauchbare Auflösungen

$x =$	0	0	1	1	2	3	3	4	5	Pferde
$y =$	11	4	12	5	6	7	0	1	2	Kühe
$z =$	31	71	11	51	31	11	51	31	11	Schafe

Beispiel 2. Eine in vollen Gulden zu 16 Ggr. zahlbare Summe Geldes lässt, wenn sie in Thalern und Gutegroschen aufgezählt wird, 1 Pfennig übrig. Welchen Betrag hat dieselbe?

Reduzirt man den Werth aller dieser Münzsorten auf Pfennige; so hat man 1 Gl. = 192 Pf., 1 Thlr. = 288 Pf., 1 Ggr. = 12 Pf. Die gesuchte Geldsumme z müsste also sowol durch $z = 192x$, als auch durch $z = 288y + 12z + 1$ darstellbar sein, und man müsste demnach $192x = 288y + 12z + 1$ oder

$$192x - 288y - 12z = 1$$

haben. Da die vier Zahlen 192, 288, 12, 1 prim sind, die drei Zahlen 192, 288, 12 aber das gemeinschaftliche Maass 12 haben; so ist die Aufgabe unmöglich.

Beispiel 3. Eine in Louisd'oren zu 5 Thlr. Gold zahl-

bare Summe Geldes lässt, wenn sie in Thalern und Gutegroschen aufgezählt wird, 6 Pfennige übrig, wenn man dabei berücksichtigt, dass das Gold $9\frac{1}{4}$ Prozent mehr werth ist, als Kurant. Wie gross ist jene Summe?

Alles auf Pfennige gebracht; so muss jene Summe, wenn sie $= x$ Louisd'oren ist, den Werth von $5.288.\frac{109\frac{1}{4}}{100}x$ Pfennigen haben, und wenn sie in Kurant aus y Thalern, z Gutegroschen und 6 Pfennigen besteht, muss sie auch $= 288y + 12z + 6$ Pfennigen sein. Man hat also

$$5.288.\frac{109\frac{1}{4}}{100}.x = 288y + 12z + 6 \text{ oder}$$

$$1311x - 240y - 10z = 5$$

Diese Aufgabe ist möglich, man darf aber, da 240 mit 1311 das gemeinschaftliche Maass 3 und mit 10 das gemeinschaftliche Maass 10 hat, nur x und z links stehen lassen. Dies giebt

$$1311x - 10z = 5 + 240y$$

worin nun y die erste Willkürliche ist.

Lös't man diese Gleichung für x und z nach §. 32 auf; so hat man $\frac{1311}{10} = [131, 10]$ also

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	131	131	1
1	10	1311	10

$$u = (-1)^{n-1}N_{n-1} = (-1)^0 N_0 = 1$$
$$v = (-1)^{n-1}M_{n-1} = (-1)^0 M_0 = 131$$

folglich als eine spezielle Auflösung der Gleichung $1311u - 10v = 1$ die Werthe $u = 1$, $v = 131$ und demnach als eine spezielle Auflösung unserer gegebenen Gleichung

$$x_1 = 1(5 + 240y) = 5 + 240y$$
$$z_1 = 131(5 + 240y) = 655 + 31440y$$

und demnach als allgemeine Auflösung unserer Gleichung

$$x = 5 + 240y + 10w$$
$$z = 655 + 31440y + 1311w$$

In diesen Ausdrücken kann man zwar dem y und w jeden beliebigen ganzen Werth geben; allein für die Anwendung in der Wirklichkeit dürfen für y nur positive Werthe gesetzt und w muss so gewählt werden, dass x und z positiv bleiben. Da man ferner bei der Geldzählung nach Thalern und Gutegroschen jeden Betrag, der gleich oder grösser als ein Thaler ist, nicht in Gutegroschen aufzählt; so wird man noch die Bedingung stellen, dass $z < 24$ sei. Diese Bedingungen werden unter Anderem erfüllt durch $y = 81$, $w = -1943$. Dies entspricht der Auflösung

$$x = 15, \ y = 81, \ z = 22$$

also der Geldsumme von 15 Louisd'oren = 81 Thlr. 22 Ggr. 6 Pf.

§. 36. Auflösung Einer Gleichung mit drei Unbekannten für den Fall, dass die Koeffizienten der Unbekannten paarweise ein gemeinschaftliches Maass haben.

I. Wenn in der vorhin betrachteten Gleichung

(1) $$ax + by + cz = k$$

nachdem die vier Koeffizienten a, b, c, k von ihrem etwaigen gemeinschaftlichen Maasse befreiet sind, die drei Koeffizienten a, b, c paarweise ein gemeinschaftliches Maass behalten; so kann man immer die Methode des §. 28 nach Vorschrift des vorhergehenden Paragraphen in Anwendung bringen, also zuvörderst

(2) $$ax + by = k - cz$$

setzen und denselben Weg einschlagen, wie wenn eine Gleichung mit den beiden Unbekannten x und y aufzulösen wäre. Der Gang dieser Rechnung wird jedoch lehren, dass unter diesen Umständen z nicht völlig willkürlich bleibt. Es werden vielmehr gleichzeitig die Nenner von x und y oder überhaupt von zwei der nach und nach mit dem Zeichen $x, y, w_1, w_2, w_3 \ldots$ auftretenden Grössen verschwinden, und man hat die Rechnung von dieser Stelle an so fortzusetzen, dass nun z Eine von denjenigen beiden Grössen wird, für welche man die fernere Auflösung bewirkt.

II. Wäre z. B.

$$6x + 10y - 15z = 7$$

gegeben; so hat man, wenn man links x und y stehen lässt,

$$6x + 10y = 7 + 15z$$

Lös't man jetzt für x auf; so kommt

$$x = \frac{7 + 15z - 10y}{6} = 1 + 2z - y + \frac{1 + 3z - 4y}{6}$$
$$= 1 + 2z - y + w_1$$
$$\frac{1 + 3z - 4y}{6} = w_1$$
$$y = \frac{1 + 3z - 6w_1}{4} = -w_1 + \frac{1 + 3z - 2w_1}{4}$$
$$= -w_1 + w_2$$
$$\frac{1 + 3z - 2w_1}{4} = w_2$$
$$w_1 = \frac{1 + 3z - 4w_2}{2} = -2w_2 + z + \frac{1 + z}{2}$$
$$= -2w_2 + z + w_3$$

Hier ist gleichzeitig der Nenner von w_1 und w_2 verschwunden und man hat, indem man nun w_3 und z als Unbekannte behandelt,

$$\frac{1 + z}{2} = w_3$$

$$z = 2w_3 - 1$$

Die rückwärts gehende Substitution liefert, indem jetzt w_2 und w_3 willkürlich bleiben,

$$x = -3 - 5w_2 + 10w_3$$
$$y = 1 - 3w_2 - 3w_3$$
$$z = -1 + 2w_3$$

III. Will man auf eine Gleichung der vorstehenden Art das Prinzip der Kettenbrüche nach §. 32 in Anwendung bringen; so hat man folgendermaassen zu verfahren.

Es sei m das grösste gemeinschaftliche Maass von a und b und $a = m\alpha$, $b = m\beta$, also α relativ prim zu β. Schreibt man jetzt die gegebene Gleichung

$$m\alpha x + m\beta y = k - cz \text{ oder}$$

(3) $$\alpha x + \beta y = \frac{k - cz}{m} = t$$

so muss offenbar $k - cz$ durch m theilbar, also t eine ganze Zahl sein.

Jetzt löse man die Gleichung $\alpha x + \beta y = t$ nach dem vorhergehenden Paragraphen auf, wobei t vorläufig völlig willkürlich bleibt. Diese Auflösung ist stets möglich, weil α und β relativ prim sind. Dieselbe ergibt für x und y Ausdrücke, welche von t und einer Willkürlichen w abhängig sind.

Hierauf löse man die Gleichung

(4) $$\frac{k - cz}{m} = t \text{ oder } mt + cz = k$$

für die beiden Unbekannten t und z auf, was ebenfalls stets möglich sein wird, weil die drei Zahlen a, b, c d. i. $m\alpha$, $m\beta$, c, also auch die beiden Zahlen m und c kein gemeinschaftliches Maass haben. Diese Auflösung ergibt für t und z Ausdrücke, welche von einer neuen Willkürlichen w_1 abhängig sind.

Substituirt man jetzt den letzteren Werth von t in die obigen Ausdrücke für x und y; so erhält man für x und y Werthe, welche von den beiden Willkürlichen w und w_1 abhängig sind, während der Werth von z nur von der Einen Willkürlichen w_1 abhängig ist.

IV. Man kann auch das Prinzip der Kettenbrüche in folgender Weise zur Lösung der vorstehenden Gleichung in Anwendung bringen. Man schreibt dieselbe

(5) $$m(\alpha x + \beta y) + cz = mt + cz = k$$

und lös't zuerst die Gleichung $mt + cz = k$ für t und z auf.

Alsdann führt man den für t gefundenen Werth in die Gleichung

(6) $$\alpha x + \beta y = t$$

ein und lös't auch diese auf.

Das letztere Verfahren ist noch etwas einfacher als das vorhin beschriebene, weil dasselbe ohne weitere Substitutionen sofort die Werthe von z, x, y ergibt.

§. 37. *Auflösung Einer Gleichung mit n Unbekannten.*

1. Das hierbei zu beobachtende Verfahren soll an dem Falle erläutert werden, wo die gegebene Gleichung $n = 5$ Unbekannte x, y, z, t, u enthält. Die Gleichung kann immer in die Form

(1) $$ax + by + cz + dt + eu = k$$

gebracht werden, worin die $n + 1$ Koeffizienten a, b, c, d, e, k ganze und relativ prime Zahlen sind.

Besitzen die n Koeffizienten a, b, c, d, e der Unbekannten ein gemeinschaftliches Maass; so ist die Auflösung unmöglich; im entgegengesetzten Falle aber stets möglich.

Die Auflösung geschieht am einfachsten in der Weise, dass man x und y links stehen lässt, die übrigen $n - 2$ Unbekannten z, t, u aber transponirt und bei der ferneren Rechnung wie bekannte, aber willkürliche Grössen behandelt. Die hierdurch entstehende Gleichung

(2) $$ax + by = k - cz - dt - eu$$

kann stets nach der Methode des §. 28, und wenn a und b relativ prim sind, auch sofort nach der Methode des §. 32 bewirkt werden, indem man beachtet, dass das früher mit k bezeichnete bekannte Glied auf der rechten Seite jetzt $k - cz - dt - eu$ ist.

Wenn a und b relativ prim sind, werden in der Auflösung die $n - 2$ Grössen z, t, u als Willkürliche erscheinen; ausserdem wird aber noch eine neue Willkürliche w, im Ganzen also deren $n - 1$ auftreten, für deren jede man eine beliebige ganze Zahl aus der Reihe $\ldots -2, -1, 0, 1, 2 \ldots$ setzen kann.

Wenn a und b ein gemeinschaftliches Maass haben, wird diese oder jene der Grössen z, t, u nicht völlig willkürlich bleiben. Für so viele der Grössen z, t, u aber, als aus der Auflösung für x und y verschwinden, werden neue Willkürliche wie $w_1, w_2 \ldots$ darin auftreten.

Wollte man in dem letzteren Falle, wo a und b ein gemeinschaftliches Maass besitzen, das Prinzip der Kettenbrüche in Anwendung bringen; so müsste man in ähnlicher Weise wie in §. 36, III oder IV gelehrt ist, verfahren.

Aus Vorstehendem erkennt man, dass die Auflösungsmethode des §. 28 mehr Elastizität besitzt, als die des §. 32, was ihr in mancher Hinsicht zur Empfehlung gereicht.

Immer werden $n - 1$ Willkürliche in die Auflösung eintreten, und man kann demnach allgemein annehmen, dass die Auflösung einer Gleichung mit n Unbekannten $x, y, z \ldots$ die Form

(3) $$\begin{cases} x = p_0 + p_1 w_1 + p_2 w_2 + \ldots + p_{n-1} w_{n-1} \\ y = q_0 + q_1 w_1 + q_2 w_2 + \ldots + q_{n-1} w_{n-1} \\ z = r_0 + r_1 w_1 + r_2 w_2 + \ldots + r_{n-1} w_{n-1} \end{cases}$$

u. s. w.

haben wird. Der Fall, wo die Eine oder andere der Unbekannten $x, y, z \ldots$ selbst, z. B. x, die Rolle einer Willkürlichen spielt, ist hierunter mit enthalten. Man würde dafür statt der obersten Gleichung einfach $x = w_1$ haben.

II. Ein Beispiel wird das Vorstehende näher erläutern Es sei für 3 Unbekannte x, y, z die Gleichung

$$6x - 4y + 5z = 17$$

gegeben. Lässt man links y und z stehen; so ergibt sich aus

$$-4y + 5z = 17 - 6x$$

in bekannter Weise nach §. 28 die Auflösung

$$(A) \quad \begin{cases} y = -3 - x + 5w \\ z = 1 - 2x + 4w \end{cases}$$

worin x und w willkürlich sind.

Lässt man links x und y stehen; so ergibt sich aus

$$6x + 5z = 17 + 4y$$

in bekannter Weise nach §. 28 die Auflösung

$$(B) \quad \begin{cases} x = 2 + 4y - 5w \\ z = 1 - 4y + 6w \end{cases}$$

worin y und w willkürlich sind.

Liesse man jedoch links x und y stehen, deren Koeffizienten 6 und -4 das gemeinschaftliche Maass 2 haben; so würde sich folgende Rechnung ergeben.

$$6x - 4y = 17 - 5z$$

$$y = \frac{-17 + 5z + 6x}{4} = -4 + z + x + \frac{-1 + z + 2x}{4}$$

$$= -4 + z + x + w_1$$

$$\frac{-1 + z + 2x}{4} = w_1$$

$$x = \frac{1 - z + 4w_1}{2} = 2w_1 + \frac{1 - z}{2} = 2w_1 + w$$

Hier verschwinden also gleichzeitig die Nenner der beiden Grössen x und w_1, für welche die Gleichung zuletzt behandelt wurde, und man hat

$$\frac{1 - z}{2} = w$$

$$z = 1 - 2w$$

und nunmehr durch rückgängige Substitution die Auflösung

$$(C) \quad \begin{cases} z = 1 - 2w \\ x = w + 2w_1 \\ y = -4 + (1 - 2w) + (2w_1 + w) + w_1 = -3 - w + 3w_1 \end{cases}$$

worin w und w_1 die beiden Willkürlichen sind.

§. 38. *Verwandlung der Willkürlichen.*

I. Jenachdem man eine Gleichung, welche mehr als zwei

Unbekannte enthält, für diese oder für jene zwei Unbekannte zuerst aufzulösen sucht, ergeben sich Auflösungen, welche eine verschiedene Zusammensetzung aus bekannten und willkürlichen Grössen zeigen.

Um nachzuweisen, dass zwei derartige Ausdrücke für Ein und dieselbe Unbekannte genau dieselbe Reihe von Zahlen darstellt, ist eine Verwandlung, Substitution oder Elimination der Willkürlichen erforderlich. Zu diesem Ende ist klar, dass wenn a_0, a_1, a_2 ... konstante Zahlen, ferner w_1, w_2, w_3 ... eine beliebige Anzahl Willkürlicher und v ebenfalls das Zeichen einer Willkürlichen ist, man im Allgemeinen nur dann

$$v = a_0 + a_1 w_1 + a_2 w_2 + a_3 w_3 + \dots$$

setzen kann, wenn unter den Koeffizienten a_1, a_2, a_3 ... irgend Einer vorkommt, welcher $= \pm 1$ ist. Denn wäre z. B. $a_1 = \pm 1$; so würde man, welchen Werth augenblicklich auch $a_0 + a_2 w_2 + a_3 w_3 + \dots$ besässe, die Grösse w_1 aus der Reihe der positiven und negativen ganzen Zahlen stets so wählen können, dass $a_0 \pm w_1 + a_2 w_2 + a_3 w_3 + \dots$ jeden beliebigen ganzen Werth v annähme.

Man wird seltener Veranlassung haben, für eine einzelne Willkürliche v den aus mehreren Willkürlichen bestehenden Ausdruck $a_0 \pm w_1 + a_2 w_2 + \dots$ zu setzen oder die Zahl der Willkürlichen zu vermehren, als umgekehrt für den letzteren Ausdruck das einfachere Zeichen v einzuführen oder die Zahl der Willkürlichen, wenn es angeht, zu vermindern.

Vermehren lässt sich diese Anzahl immer, indem, wenn $a_0 \pm w_1 + a_2 w_2 + \dots$ für v gesetzt wird, w_1, w_2 ... vollkommen willkürlich gedacht werden können.

Vermindern lässt sich die fragliche Anzahl jedoch in den meisten Fällen nicht. Denn man muss beachten, dass wenn v für $a_0 \pm w_1 + a_2 w_2 + \dots$ gesetzt wird, zwischen den Grössen v, w_1, w_2, ... die durch die Gleichung $v = a_0 \pm w_1 + a_2 \cdot w_2 + \dots$ ausgedrückte Beziehung besteht, wodurch nunmehr die Grössen v, w_1, w_2 ... nicht sämmtlich willkürlich bleiben, vielmehr voneinander abhängig werden. Unter diesen Umständen würde es unzulässig sein, die Grössen v, w_1, w_2 ..., wenn sie noch an anderen Stellen der zusammengehörigen Formeln erscheinen, immer wieder aufs Neue als Willkürliche zu betrachten, um dieselben durch Substitutionen der vorstehenden Art endlich bis auf Eine ganz aufzureiben. Man hat vielmehr zu berücksichtigen, dass wenn man $v = a_0 \pm w_1 + a_2 w_2 + \dots$ setzt, auch fernerhin die Grössen w_2, w_3 ... willkürlich bleiben, von den beiden Grössen v und w_1 jedoch nur Eine willkürlich bleibt, während die andere durch die letztere Bedingungsgleichung von der ersteren und von w_2, w_3 ... abhängig wird.

So kann man z. B. in der Formel $x = 2w + 2w_1$ unbe-

denklich $w + w_1 = v$ also $x = 2v$ setzen, wodurch die Zahl der Willkürlichen um Eine vermindert ist.

Man kann jedoch durch keine Substitution bewirken, dass x als eine einfache Willkürliche v erscheint. Denn setzte man z. B. erst $x = w + w + 2w_1$, und nun $w + 2w_1 = v$ also $x = w + v$; so müsste man beachten, dass in der Gleichung $w + 2w_1 = v$ wol w_1 willkürlich bleibt, dass aber von w und v nur Eine willkürlich bleiben kann. Nimmt man also v als Willkürliche; so darf nicht auch w als Willkürliche in der Formel für x stehen bleiben, man muss vielmehr $w = v - 2w_1$ also $x = v - 2w_1 + v = 2v - 2w_1$ setzen.

Dagegen kann der Werth $x = 2w + 3w_1$ als einfache Willkürliche erscheinen. Denn schreibt man $x = 2(w + w_1) + w_1$; so kann man zuvörderst $w + w_1 = v$ also $x = 2v + w_1$ setzen. Hierbei kann entweder v und w oder v und w_1 als Willkürlich betrachtet werden. Nimmt man $v + w_1$ als Willkürlich an; so kann $2v + w_1 = v_1$ also $x = v_1$ gesetzt werden.

II. Wenden wir die vorstehenden Betrachtungen darauf an, um zu zeigen, dass die drei Auflösungen (A), (B), (C) im vorhergehenden Paragraphen ganz dieselben Zahlen vorstellen.

Aus dem Systeme (C) erkennt man, dass die Grösse x, weil sie von der Form $w + 2w_1$ ist, als Willkürliche angenommen werden kann. Alsdann hat man $w = x - 2w_1$ und wenn Dies in die Ausdrücke für y und z substituirt wird,

$$y = -3 - x + 5w_1$$
$$z = 1 - 2x + 4w_1$$

Hierdurch erhält man das System (A).

Aus dem Systeme (C) erkennt man ferner, dass auch die Grösse y, weil sie von der Form $-3 - w + 3w_1$ ist, zur Willkürlichen angenommen werden kann. Geschieht Dies; so hat man $w = -3 - y + 3w_1$, worin w_1 willkürlich bleibt. Substituirt man diesen Werth in die Ausdrücke für x und z; so kommt

$$x = -3 - y + 5w$$
$$z = 7 + 2y - 6w$$

Diese beiden Ausdrücke können, wenn man für $1 + y - w$ das Zeichen v einer neuen Willkürlichen setzt, in die Form

$$x = 2 + 4y - 5(1 + y - w) = 2 + 4y - 5v$$
$$z = 1 - 4y + 6(1 + y - w) = 1 - 4y + 6v$$

gebracht werden, in welcher sie dem Systeme (B) entsprechen.

§. 39. *Auflösung von r Gleichungen mit n Unbekannten.*

Das Verfahren soll an dem Falle erläutert werden, wo $n = 4$ Gleichungen mit $r = 7$ Unbekannten $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ gegeben sind. Diese 4 Gleichungen seien

$$\begin{aligned}
(1)\ & a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 + a_5 x_5 + a_6 x_6 + a_7 x_7 = a_0 \\
(2)\ & b_1 x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4 + b_5 x_5 + b_6 x_6 + b_7 x_7 = b_0 \\
(3)\ & c_1 x_1 + c_2 x_2 + c_3 x_3 + c_4 x_4 + c_5 x_5 + c_6 x_6 + c_7 x_7 = c_0 \\
(4)\ & d_1 x_1 + d_2 x_2 + d_3 x_3 + d_4 x_4 + d_5 x_5 + d_6 x_6 + d_7 x_7 = d_0
\end{aligned}$$

Die Aufgabe ist zunächst dann unmöglich, wenn, nachdem alle 8 Koeffizienten einer jeden Gleichung, wie a_1, $a_2 \ldots a_7$, a_0, von ihrem gemeinschaftlichen Maasse befreiet sind, die 7 Koeffizienten a_1, $a_2 \ldots a_7$ der Unbekannten noch ein gemeinschaftliches Maass besitzen.

Findet dieser Fall der Unmöglichkeit nicht statt; so lös't man die Gl. (1) nach §. 37 wie eine Gleichung mit $n = 7$ Unbekannten auf. Dies gibt

(5) $x_1, x_2 \ldots x_7$ ausgedrückt durch $n - 1 = 6$ Willkürliche $t_1, t_2 \ldots t_6$

Diese Werthe von x_1, $x_2 \ldots x_7$ substituirt man in Gl. (2), wodurch man eine Gleichung mit $n - 1 = 6$ Unbekannten t_1, $t_2 \ldots t_6$ erhält.

Lös't man hierauf die letztere Gleichung nach §. 37 auf; so ergibt sich

(6) $t_1, t_2 \ldots t_6$ ausgedrückt durch $n - 2 = 5$ Willkürliche $u_1, u_2 \ldots u_5$

Nun setzt man erst diese Werthe von t_1, $t_2 \ldots t_6$ in die Ausdrücke (5), wodurch man

(7) $x_1, x_2 \ldots x_7$ ausgedrückt durch $n - 2 = 5$ Willkürliche $u_1, u_2 \ldots u_5$

erhält. Durch diese Werthe der ursprünglichen Unbekannten werden die ersten beiden gegebenen Gleichungen erfüllt.

Die letzteren Werthe von x_1, $x_2 \ldots x_7$ substituirt man in Gl. (3), wodurch man eine Gleichung mit $n - 2 = 5$ Unbekannten u_1, $u_2 \ldots u_5$ erhält.

Lös't man diese Gleichung nach §. 37 auf; so ergibt sich

(8) $u_1, u_2 \ldots u_5$ ausgedrückt durch $n - 3 = 4$ Willkürliche v_1, v_2, v_3, v_4

Diese Werthe von u_1, $u_2 \ldots u_5$ setzt man erst in die Ausdrücke (7), wodurch man

(9) $x_1, x_2 \ldots x_7$ ausgedrückt durch $n - 3 = 4$ Willkürliche v_1, v_2, v_3, v_4

erhält. Durch diese Werthe der ursprünglichen Unbekannten werden die ersten drei gegebenen Gleichungen erfüllt.

Die vorstehenden Werthe von x_1, $x_2 \ldots x_7$ substituirt man in die letzte Gleichung (4), wodurch man eine Gleichung mit $n - 3 = 4$ Unbekannten v_1, v_2, v_3, v_4 erhält.

Lös't man diese Gleichung nach §. 37 auf; so ergibt sich

(10) v_1, v_2, v_3, v_4 ausgedrückt durch $n - r = 3$ Willkürliche w_1, w_2, w_3

Substituirt man diese Werthe von v_1, v_2, v_3, v_4 in die Ausdrücke (9); so erhält man die gesuchten Werthe von

(11) $x_1, x_2 \ldots x_7$ ausgedrückt durch $n - r = 3$ Willkürliche w_1, w_2, w_3

welche allen gegebenen $r = 4$ Gleichungen ein Genüge leisten.

Sollte man bei der Auflösung der Gleichungen (1), (2), (3), (4) auf einen unmöglichen Fall stossen; so ist die ganze Aufgabe unmöglich.

§. 40. Beispiele.

Beispiel 1. Es seien folgende 2 Gleichungen mit 3 Unbekannten x, y, z gegeben

(1) $2x - 5y + 4z = 3$

(2) $3x + 7y - 8z = 6$

Eine Auflösung der ersten (nach §. 37 und 28 für x und y bewirkt) gibt

(3) $x = -1 - 2z + 5v \quad y = -1 + 2v \quad z = z$

Substituirt man diese Werthe in Gl. (2); so erhält man

(4) $-14z + 29v = 16$

Eine Auflösung dieser Gleichung (nach §. 37 und 28 bewirkt) gibt

(5) $z = 3 + 29w \quad v = 2 + 14w$

Substituirt man diese Werthe in die Ausdrücke (3); so erhält man die Auflösung der gegebenen Gleichungen in der Form

(6) $x = 3 + 12w \quad y = 3 + 28w \quad z = 3 + 29w$

Hiernach hat man unter Anderem folgende spezielle Auflösungen

für $w =$	...	-2	-1	0	1	2	...
$x =$	...	-21	-9	3	15	27	...
$y =$	...	-53	-25	3	31	59	...
$z =$	...	-55	-26	3	32	61	...

Beispiel 2. Es seien folgende 3 Gleichungen mit den 4 Unbekannten x, y, z, t gegeben:

(1) $3x + 5t = 19$

(2) $-7y + 4t = 1$

(3) $4z + 3t = -6$

Die Auflösung der Gl. (1) (nach §. 37 und 28 bewirkt) gibt

(4) $x = 8 - 5u \quad t = -1 + 3u$

Durch Substitution dieser Werthe in Gl. (2) kommt

(5) $-7y + 12u = 5$

Die Auflösung dieser Gleichung (nach §. 37 und 28 bewirkt) gibt

(6) $y = 1 + 12v \quad u = 1 + 7v$

Durch Einführung dieser Werthe in die Formeln (4) erhält man

(7) $x = 3 - 35v \quad y = 1 + 12v \quad t = 2 + 21v$

wodurch die beiden Gleichungen (1) und (2) erfüllt werden.

Substituirt man die letzteren Werthe in Gl. (3); so kommt

(8) $4z + 63v = -12$

und durch Auflösung dieser Gleichung nach §. 37 und 28

(9) $z = -3 - 63w \quad v = 4w$

Die Einführung dieser Werthe in die Ausdrücke (7) führt zu der gesuchten Auflösung

(10) $x = 3 - 140w \quad y = 1 + 48w \quad z = -3 - 63w \quad t = 2 + 84w$

odurch alle gegebenen 3 Gleichungen erfüllt werden.

Beispiel 3. Es seien folgende 2 Gleichungen mit den 4 Unbekannten x, y, z, u gegeben:

(1) $4x + 3y + 8z + 12u = 126$

(2) $8x - 3y + z + 18u = 15$

Die Auflösung der Gl. (1) (nach §. 37 und 28 für x und y bewirkt) gibt

(3) $x = -2z - v \quad y = 42 - 4u + 2v \quad z = z \quad u = u$

Durch Substitution dieser Werthe in Gl. (2) kommt

(4) $-15z + 30u - 14v = 141$

Die Auflösung dieser Gleichung (nach §. 37 und 28 für z und u bewirkt) gibt

(5) $z = -15 + 2u - 14w \quad u = u \quad v = 6 + 15w$

Führt man diese Werthe in die Ausdrücke (3) ein; so ergibt sich die gesuchte Auflösung in der Form

(6) $\begin{cases} x = 24 - 4u + 13w & y = 54 - 4u + 30w \\ z = -15 + 2u - 14w & u = u \end{cases}$

Im vorstehenden Beispiele wäre es jedoch zweckmässiger gewesen, erst die Gl. (2) für z aufzulösen. Dies gibt sofort

(7) $x = x \quad y = y \quad z = 15 - 8x + 3y - 18u \quad u = u$

und wenn man diese Werthe in Gl. (1) substituirt,

(8) $-20x + 9y - 44u = 2$

Eine Auflösung dieser Gleichung (nach §. 37 und 28 für x und y bewirkt) gibt

(9) $x = -1 - 4u + 9w \quad y = -2 - 4u + 20w \quad u = u$

Substituirt man diese Werthe in die Ausdrücke (7); so erhält man die gesuchte Auflösung in der Form

(10) $\begin{cases} x = -1 - 4u + 9w & y = -2 - 4u + 20w \\ z = 17 + 2u - 12w & u = u \end{cases}$

Hiernach hat man unter Anderem für $u = 1$, $w = 1$ die spezielle Auflösung

$$x = 4 \quad y = 14 \quad z = 7 \quad u = 1$$

§. 41. *Beiläufige Anmerkung für die bestimmte Algebra.*

Das dem Verfahren in §. 39 zu Grunde liegende Prinzip kann auch zur Auflösung von n bestimmten Gleichungen mit n Unbekannten verwendet werden, und dürfte sich besonders dazu eignen, um den Zweck und die Nothwendigkeit der zur Auflösung führenden Operationen möglichst anschaulich zu machen.

Wenn hiernach etwa für $n = 4$ zwischen den 4 Unbekannten x_1, x_2, x_3, x_4 die 4 Gleichungen

(1) $a_0 + a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 = 0$

(2) $b_0 + b_1 x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4 = 0$

(3) $c_0 + c_1 x_1 + c_2 x_2 + c_3 x_3 + c_4 x_4 = 0$

(4) $d_0 + d_1 x_1 + d_2 x_2 + d_3 x_3 + d_4 x_4 = 0$

gegeben sind; so lös't man zuvörderst Gl. (1) für Eine der Unbekannten, z. B. für x_4 auf. Dies gibt

(5) $$x_4 = F_1(x_1, x_2, x_3)$$

Durch diesen Werth von x_4 und jeden beliebigen von x_1, x_2, x_3 wird die erste Gleichung erfüllt.

Substituirt man diesen Werth von x_4 in Gl. (2); so erhält man eine Gleichung mit den $n - 1 = 3$ Unbekannten x_1, x_2, x_3 in der Form

(6) $$e_0 + e_1 x_1 + e_2 x_2 + e_3 x_3 = 0$$

Lös't man diese Gleichung für x_3 auf; so kommt

$$x_3 = F_2(x_1, x_2)$$

und wenn man diesen Werth in den Ausdruck (5) einführt, und den vorstehenden Werth von x_3 daneben schreibt,

(7) $$x_3 = F_2(x_1, x_2) \qquad x_4 = F_3(x_1, x_2)$$

Durch diese Werthe von x_3, x_4 und jeden beliebigen von x_1, x_2 werden die ersten zwei Gleichungen erfüllt.

Substituirt man diese Werthe von x_3, x_4 in Gl. (3); so erhält man eine Gleichung mit $n - 2 = 2$ Unbekannten x_1, x_2 in der Form

(8) $$f_0 + f_1 x_1 + f_2 x_2 = 0$$

Lös't man dieselbe für x_2 auf; so kommt

$$x_2 = F_4(x_1)$$

und wenn man diesen Werth in die Ausdrücke (7) einführt und den vorstehenden Werth von x_2 daneben schreibt,

(8) $$x_2 = F_4(x_1) \qquad x_3 = F_5(x_1) \qquad x_4 = F_6(x_1)$$

Durch diese Werthe von x_2, x_3, x_4 und jeden beliebigen von x_1 werden die ersten drei Gleichungen erfüllt.

Substituirt man endlich diese Werthe von x_2, x_3, x_4 in die letzte Gl. (4); so erhält man eine Gleichung mit nur Einer Unbekannten x_1 in der Form

(9) $$g_0 + g_1 x_1 = 0$$

Lös't man dieselbe auf; so erhält man für x_1 einen bestimmten Werth h.

Führt man denselben in die Ausdrücke (8) ein; so ergibt sich die gesuchte Auflösung in der Form

(10) $$x_1 = h \qquad x_2 = F_4(h) \qquad x_3 = F_5(h) \qquad x_4 = F_6(h)$$

Durch diese Werthe von x_1, x_2, x_3, x_4 werden alle gegebenen $n = 4$ Gleichungen erfüllt.

Dritter Abschnitt.

Theorie der Ungleichheiten vom ersten Grade.

Erste Auflösungsmethode.

§. 42. *Allgemeine Begriffe.*

I. Die Auflösung der unbestimmten Gleichungen vom ersten Grade führt zu Ausdrücken für die Unbekannten x, y ..., welche von gewissen Willkürlichen w, w_1 ..., die selbst nur vom ersten Grade darin vorkommen, abhängig sind.

Häufig werden an die unbekannten Grössen noch besondere Bedingungen gestellt, namentlich die, dass sie zwischen gewissen Gränzen liegen sollen, z. B. indem man verlangt, dass x zwischen 10 und 100 liege, oder dass sie jenseit einer gegebenen Gränze liegen sollen, z. B. indem man verlangt, dass x positiv, d. h. > 0 sei. Hierdurch vermindert sich die unendliche Menge der sonst möglichen Auflösungen; zuweilen bleibt nur eine endliche Reihenfolge derselben zulässig, zuweilen nur eine einzige, sodass die unbestimmte Aufgabe den Charakter einer bestimmten annimmt; zuweilen wird sogar durch jene Bedingung die Aufgabe unmöglich gemacht.

Die Aufgaben in §. 33 und 35 enthalten einige praktische Beispiele solcher Nebenbedingungen, und man wird sich besonders in §. 35 überzeugt haben, dass die Aufsuchung der zulässigen Auflösung durch tabellarische Berechnung der allgemeinen Werthe für x, y ..., wobei man die Willkürlichen w, w_1 ... beliebig variiren lässt, im hohen Grade mühsam werden kann.

Es kommt also auf eine direkte Methode zur Bestimmung der engsten Gränzen an, innerhalb welcher die Willkürlichen w, w_1 ... gehalten werden müssen, um die einzig zulässigen Auflösungen zu ergeben.

II. Die Werthe der Unbekannten x, y ... ergeben sich allgemein in der Form

(1) $$x = p_1 + q_1 w + r_1 w_1 + \dots$$

(2) $$y = p_2 + q_2 w + r_2 w_1 + \dots$$

u. s. w.

Die Bedingungen für die Gränzen von $x, y \ldots$ werden im Allgemeinen immer paarweise in der Form

(3) $x > \alpha_1 \qquad x < \beta_1$

(4) $y > \alpha_2 \qquad y < \beta_2$

u. s. w. gegeben sein. Wäre für eine Unbekannte x nur auf der Einen Seite eine Gränze gegeben; so fällt allerdings hierfür die Eine Ungleichheit aus: man kann übrigens, wenn man will, für die zweite Gränze resp. den Werth $+\infty$ oder $-\infty$ setzen, um dadurch das Paar zu vervollständigen. Ebenso könnte man, wenn für eine Unbekannte keinerlei Gränze gegeben wäre, entweder das betreffende Paar ganz weglassen, oder dafür $x > -\infty$ $x < +\infty$ schreiben.

Setzt man in die Ungleichheiten (3), (4) für x, y die Werthe (1), (2); so erhält man die Ungleichheiten

(5) $p_1 + q_1 w + r_1 w_1 + \ldots > \alpha_1 \qquad p_1 + q_1 w + r_1 w_1 + \ldots < \beta_1$

(6) $p_2 + q_2 w + r_2 w_1 + \ldots > \alpha_2 \qquad p_2 + q_2 w + r_2 w_2 + \ldots < \beta_2$

u. s. w., woraus die Gränzen der Grössen $w, w_1 \ldots$ zu bestimmen sind.

Die hieraus paarweise für $w, w_1 \ldots$ sich ergebenden Gränzwerthe wollen wir die Auflösungen der gegebenen Ungleichheiten nennen.

In den folgenden Paragraphen werden wir uns mit der Auflösung solcher Ungleichheiten durch direkte Methoden, welche manches Ähnliche mit der Auflösung bestimmter Gleichungen haben, beschäftigen, und schicken zu dem Ende folgende Bemerkungen voraus.

III. In Absicht auf die unbestimmten Gleichungen müssen allerdings die Grössen $w, w_1 \ldots$ für welche die Ungleichheiten aufzulösen sind, ganze Zahlen sein. Bei der allgemeinen Behandlung der Ungleichheiten werden jedoch jene Grössen als beliebig veränderlich gedacht. Am Schlusse der Rechnung wird es leicht sein, die besonderen Anforderungen wegen der unbestimmten Gleichungen zu berücksichtigen. Fände man z. B. $5\frac{3}{4}$ und $8\frac{1}{2}$ als genaue Gränzwerthe von w; so wären für die unbestimmten Gleichungen 6 und 8 die betreffenden ganzen Gränzwerthe für w, und es könnte w nur $= 6, 7, 8$ sein.

IV. Jeder aus der stetigen Reihe der negativen und positiven Grössen von $-\infty$ bis $+\infty$ entnommene Werth heisst grösser, als jeder links davon liegende; also z. B. $15 > 2 > 0 > -3 > -20$.

Wenn mithin in der Ungleichheit $a > b$ die beiden Grössen a und b positiv sind; so muss der absolute Werth von a grösser als der von b sein; wenn aber a und b negativ sind, muss der absolute Werth von a kleiner als der von b sein. Wenn a und b verschiedene Zeichen haben, kann nur a positiv und b negativ sein; der absolute Werth von a kann aber sowol grösser, wie kleiner, als der von b sein.

§. 43. Die Grundoperationen mit Ungleichheiten.

Die einfachsten Umformungen, welche man mit Ungleichheiten vornehmen kann, sind folgende:

I. Die beiden Ungleichheiten $a > b$ und $b < a$, von denen die Eine durch Umkehrung der anderen entsteht, sind gleichbedeutend.

II. Man kann auf beiden Seiten einer Ungleichheit Ein und dieselbe Grösse addiren oder subtrahiren, und mithin auch die Glieder einer Ungleichheit transponiren. Wenn also $a > b$; so ist auch $a \pm c > b \pm c$, worin gleichzeitig die oberen oder die unteren Zeichen gelten. Wenn $a - b + c > d + e - f$; so ist durch Transposition auch $a + c + f > b + d + e$. Wenn $a > b$; so ist durch Transposition beider Seiten $-b > -a$. Durch Transposition der Einen Seite kann man jede Ungleichheit $a > b$ nach Art der Gleichungen annulliren oder auf null reduziren, also in die Form $a - b > 0$ oder auch in die Form $b - a < 0$ bringen.

III. Zwei Ungleichheiten können so addirt werden, dass in beiden das Grössere auf derselben Seite steht. Wenn also $a > b$ und $c > d$; so ist auch $a + c > b + d$.

IV. Subtrahirt kann von einer Ungleichheit eine andere nur in der Weise werden, dass von dem Grösseren der Einen das Kleinere der anderen subtrahirt wird, indem das Ungleichheitszeichen der Differenz gleich dem des Minuends wird. Wenn also $a > b$ und $c > d$ oder $d < c$; so ist auch $a - d > b - c$.

V. Man kann die beiden Seiten einer Ungleichheit mit einer positiven Zahl multipliziren oder dividiren. Multiplizirt oder dividirt man aber mit einer negativen Zahl; so muss das Ungleichheitszeichen umgekehrt werden. Wenn also $a > b$ und m positiv ist; so hat man $ma > mb$, und $\frac{a}{m} > \frac{b}{m}$; dagegen $-ma < -mb$ und $\frac{a}{-m} < \frac{b}{-m}$. Wenn man also die Zeichen aller Glieder einer Ungleichheit umkehren will; so muss man auch das Ungleichheitszeichen umkehren.

VI. Wenn zwei Ungleichheiten miteinander multiplizirt werden sollen; so müssen im Allgemeinen die beiden Seiten einer jeden gleiche Zeichen haben. Das Resultat ist, wenn a, b, c, d absolute Werthe bezeichnen, aus Folgendem zu ersehen:

$$\begin{array}{c} a > b \\ c > d \\ \hline ac > bd \end{array} \qquad \begin{array}{c} -b > -a \\ -d > -c \\ \hline bd < ac \end{array} \qquad \begin{array}{c} a > b \\ -c < -d \\ \hline -ac < -bd \end{array} \qquad \begin{array}{c} b < a \\ -d > -c \\ \hline -bd > -ac \end{array}$$

VII. Für die Division zweier Ungleichheiten durch einander, wofür derselbe Vorbehalt, wie bei der Multiplikation gemacht wird, hat man

$$\begin{array}{cccc} a>b & -b>-a & a>b & b<a \\ d<c & -c<-d & -d>-c & -c<-d \\ \hline \frac{a}{d}>\frac{b}{c} & \frac{b}{c}<\frac{a}{d} & -\frac{a}{d}<-\frac{b}{c} & -\frac{b}{c}>-\frac{a}{d} \end{array}$$

VIII. In jeder Ungleichheit kann man für einzelne darin vorkommende Grössen andere von verschiedenem Werthe substituiren, so jedoch, dass dadurch die grössere Seite der Ungleichheit vergrössert, oder die kleinere verkleinert wird.

Wäre z. B., wenn $a, b, c\ldots$ absolute Werthe bezeichnen, $a+\frac{b}{c}>\frac{d}{e}-f$ gegeben; so hätte man auch,

$$\begin{array}{llll} \text{wenn} & x>a & \text{ist,} & x+\frac{b}{c}>\frac{d}{e}-f \\ » & x>f & » & a+\frac{b}{c}>\frac{d}{e}-x \\ » & x>b & » & a+\frac{x}{c}>\frac{d}{e}-f \\ » & x>e & » & a+\frac{b}{c}>\frac{d}{x}-f. \end{array}$$

IX. Wenn in einer Ungleichheit $A>B$ veränderliche oder unbekannte Grössen vorkommen; so sind diejenigen Werthe der Veränderlichen, für welche $A=B$ wird, die Gränzwerthe der Letzteren. Zuweilen verlangt man, dass diese Gränzwerthe selbst mit ausgeschlossen sein sollen, was der strengen Bedeutung der Ungleichheit $A>B$ entspricht. Zuweilen jedoch sollen die Gränzwerthe selbst mit zulässig sein. Für diesen Fall müsste man eigentlich $A\geqq B$ schreiben. Wir werden indessen der Einfachheit wegen die Formel $A>B$ in beiden Fällen beibehalten, und die leicht sich ergebenden Bemerkungen für den Fall, wo auch $A=B$ sein kann, besonders angeben oder dem Leser überlassen. Hätte man also nur mit ganzen Zahlen zu thun, und sollten z. B. unter x alle positiven ganzen Zahlen mit Einschluss der Null verstanden werden; so würde man bei Zulassung der Gränzwerthe $x>0$, dagegen bei Verwerfung der Gränzwerthe $x>-1$ schreiben.

§. 44. *Auflösung Einer Ungleichheit mit Einer Veränderlichen.*

Wenn nur Eine Ungleichheit mit der Veränderlichen w in der Form

(1) $$p+qw>\alpha$$

gegeben ist; so folgt daraus zunächst durch Transposition des bekannten Gliedes p

$$qw>\alpha-p$$

Um aber die Gränze für w zu bestimmen, kommt es darauf an, ob der Koeffizient q von w positiv oder negativ ist. Ist q positiv; so ergibt sich durch Division mit q

(2) $$w > \frac{\alpha - p}{q}.$$

Ist dagegen q negativ; so ergibt sich durch diese Division

(3) $$w < \frac{\alpha - p}{q}.$$

In beiden Fällen kann also durch die gegebene Ungleichheit die Reihe der für die Veränderliche w zu setzenden Zahlen nur auf Einer Seite begränzt werden.

Wäre die Ungleichheit $p + qw < \alpha$ gegeben; so würden sich in der vorstehenden Auflösung nur die Ungleichheitszeichen umkehren.

Beispiel. Im zweiten Beispiele des §. 33 wurde verlangt, dass die Grösse z, deren Werth sich in der Form $31 + 60w$ ergab, nur positiv sein sollte. Rechnet man zu diesen Zahlen auch die Null; so hat man bei Zulassung der Gränzwerthe die Bedingung

$$31 + 60w > 0 \text{ also}$$
$$w > -\frac{31}{60}.$$

Da es nun hier bloss auf ganze Zahlen ankommt; so muss $w > 0$ genommen werden, was sich auch bereits in §. 33 bestätigt hat.

§. 45. *Auflösung Eines Paares von Ungleichheiten mit Einer Veränderlichen.*

Ein Paar von Ungleichheiten nennen wir zwei Ungleichheiten, nach deren erster ein Ausdruck grösser und nach deren zweiter derselbe Ausdruck kleiner sein soll, als gewisse bekannte Grössen.

Wir haben also hier zwei Ungleichheiten wie

(1) $$p + qw > \alpha \qquad p + qw < \beta$$

zu betrachten, worin offenbar $\beta > \alpha$ sein muss.

Durch Transposition von p folgt daraus

$$qw > \alpha - p \qquad qw < \beta - p$$

Ist nun q positiv; so ergibt eine Division mit q die Auflösung

(2) $$w > \frac{\alpha - p}{q} \qquad w < \frac{\beta - p}{q}$$

Ist dagegen q negativ; so erhält man die Auflösung

(3) $$w < \frac{\alpha - p}{q} \qquad w > \frac{\beta - p}{q}$$

In beiden Fällen wird hierdurch für w eine untere und eine obere Gränze bestimmt.

Da $\beta > \alpha$ ist; so leuchtet ein, dass auch stets der hiernach gefundene obere Gränzwerth von w grösser ist, als der gefundene untere Gränzwerth.

Beispiel. Verlangte man in dem Beispiele des vorhergehenden Paragraphen für $z = 31 + 60w$ die zwischen 100 und 500 liegenden Werthe; so hätte man

$$31 + 60w > 100 \qquad 31 + 60w < 500$$

also

$$w > \frac{69}{60} \qquad w < \frac{469}{60}$$

oder

$$w > 1\frac{9}{60} \qquad w < 7\frac{49}{60}$$

Da nun für die diophantische Aufgabe w eine ganze Zahl sein muss; so hat man bei Zulassung der Gränzwerthe $w > 2$, $w < 7$, sodass also für w die Werthe 2, 3, 4, 5, 6, 7 zu nehmen sind.

§. 46. *Auflösung beliebig vieler vollständigen und unvollständigen Paare von Ungleichheiten mit Einer Veränderlichen.*

I. Es seien beliebig viele, z. B. 3 Paar Ungleichheiten mit der Veränderlichen w in der Form

(1) $\quad p_1 + q_1 w > \alpha_1 \qquad p_1 + q_1 w < \beta_1$

(2) $\quad p_2 + q_2 w > \alpha_2 \qquad p_2 + q_2 w < \beta_2$

(3) $\quad p_3 + q_3 w > \alpha_3 \qquad p_3 + q_3 w < \beta_3$

gegeben. Es kann auch von diesem oder jenem Paare die Eine Hälfte fehlen, in welchem Falle wir dasselbe ein unvollständiges Paar nennen.

Lös't man jede Ungleichheit nach §. 44 für w auf; so erhält man ebenso viel vollständige oder unvollständige Paare von Auflösungen, als Paare von Ungleichheiten gegeben sind, hier also 3, welche wir kurz

(4) $\quad w > A_1 \qquad w < B_1$

(5) $\quad w > A_2 \qquad w < B_2$

(6) $\quad w > A_3 \qquad w < B_3$

schreiben wollen.

II. Jetzt muss offenbar jeder obere Gränzwerth B_1, B_2, B_3 von w grösser sein, als jeder untere Gränzwerth A_1, A_2, A_3. Wäre Dies nicht der Fall; so würde die Aufgabe unmöglich sein.

Dass nun aber in jedem vollständigen Paare (4), (5), (6) der Auflösungen, welches sich aus einem vollständigen Paare der gegebenen Ungleichheiten ergeben hat, die obere Gränze grösser ist, als die untere, folgt schon aus §. 45. Die Bedingungen $B_1 > A_1$, $B_2 > A_2$, $B_3 > A_3$ realisiren sich also von selbst,

insofern nur in den gegebenen Ungleichheiten $\beta_1 > \alpha_1$, $\beta_2 > \alpha_2$, $\beta_3 > \alpha_3$ ist. Dieselben brauchen also nicht weiter berücksichtigt zu werden.

Man muss aber ferner, damit die Aufgabe möglich sei, haben

$$B_1 > A_2 \qquad B_2 > A_1 \qquad B_3 > A_1$$
$$B_1 > A_3 \qquad B_2 > A_3 \qquad B_3 > A_2$$

oder auch

(7) $B_1 > A_2 \qquad A_1 < B_2$

(8) $B_1 > A_3 \qquad A_1 < B_3$

(9) $B_2 > A_3 \qquad A_2 < B_3$

III. Was nun die gesuchten Gränzwerthe von w betrifft; so ist offenbar die grösste oder das Maximum der Zahlen A_1, A_2, A_3, welches wir mit A bezeichnen wollen, der untere Gränzwerth, und die kleinste oder das Minimum der Zahlen B_1, B_2, B_3, welches wir mit B bezeichnen wollen, der obere Gränzwerth. Man hat also als Auflösung der gegebenen Ungleichheiten

(10) $w > A \qquad w < B$

Die Unmöglichkeit der Aufgabe liegt vor, wenn das Maximum A grösser ist, als das Minimum B.

Wäre irgend ein Paar (4), (5) oder (6) unvollständig; so kommt die fehlende Hälfte nicht in Betracht. Man kann übrigens eine fehlende linke Hälfte durch $w > -\infty$ und eine fehlende rechte Hälfte durch $w < +\infty$ ergänzen.

Es ist klar, dass die gegebenen Ungleichheiten (1), (2), (3) nicht bloss die gefundenen Bedingungen (10) nothwendig erfordern, sondern dass auch eine Erfüllung dieser letzteren Bedingungen nothwendig die Verwirklichung der gegebenen Ungleichheiten zur Folge hat.

Beispiel 1. Es seien folgende 3 Paar Ungleichheiten gegeben:

$$2 + 7w > 5 \qquad 2 + 7w < 30$$
$$15 - 3w > 1 \qquad 15 - 3w < 25$$
$$6w > -4 \qquad 6w < 17$$

Hieraus folgt zuvörderst

$$w > \tfrac{3}{7} \qquad w < 4$$
$$w > -3\tfrac{1}{3} \qquad w < 4\tfrac{2}{3}$$
$$w > -\tfrac{2}{3} \qquad w < 2\tfrac{5}{6}$$

Die Aufgabe ist möglich, und man hat

$$w > \tfrac{3}{7} \qquad w < 2\tfrac{5}{6},$$

folglich in ganzen Zahlen mit Zulassung der Gränzwerthe

$$w > 0 \qquad w < 2$$

sodass für w die Zahlen 0, 1, 2 zu setzen sind.

Beispiel 2. Im ersten Beispiele §. 33 wurde verlangt, dass $x = 600 - 4w$ und $y = -4800 + 33w$ positive Zahlen,

einschliesslich der Null seien. Man hat also hier 2 unvollständige Paare von Ungleichheiten, nämlich

$$600 - 4w > 0 \quad \ldots\ldots$$
$$-4800 + 33w > 0 \quad \ldots\ldots$$

Hiernach muss sein

$$\ldots\ldots \qquad w < 150$$
$$w > 145\tfrac{5}{11} \qquad \ldots\ldots$$

Die gesuchte Auflösung ist also

$$w > 145\tfrac{5}{11} \qquad w < 150$$

folglich in ganzen Zahlen

$$w > 146 \qquad w < 150$$

sodass für w die Zahlen 146, 147, 148, 149, 150 zu setzen sind, was sich auch schon in §. 33 gezeigt hat.

Beispiel 3. Würde im vorstehenden Beispiele verlangt, dass x positiv und y negativ sei; so hätte man

$$600 - 4w > 0 \qquad \ldots\ldots$$
$$\ldots\ldots \qquad -4800 + 33w < 0$$

Hieraus ergibt sich

$$\ldots\ldots \qquad w < 150$$
$$\ldots\ldots \qquad w < 145\tfrac{5}{11}$$

Demnach hat man für w bloss die Eine Gränze $w < 145\tfrac{5}{11}$ oder die ganzen Zahlen $w < 145$.

§. 47. *Elimination der Veränderlichen aus Ungleichheiten.*

Wenn A und B zwei Ausdrücke sind, welche mehrere Veränderliche w, w_1, w_2 ... enthalten, und es darauf ankommt, aus den beiden Ungleichheiten

(1) $$A \gtrless 0$$

(2) $$B \gtrless 0$$

Eine Unbekannte w zu eliminiren, also eine Ungleichheit herzustellen, welche nur noch die übrigen Unbekannten w_1, w_2 ... enthält; so kann Dies, wenn es überhaupt thunlich ist, ähnlich wie bei den Gleichungen, auf mehrfache Weise geschehen.

I. Nach dem Prinzipe der Kombination. — Man lös't nach §. 44 sowol die Ungleichheit (1), wie auch die Ungleichheit (2) für w auf. Erhält man hierdurch zwei Ungleichheiten mit verschiedenen Ungleichheitszeichen, also

(3) $$w > C \qquad w < D$$

so ist durch Kombination derselben

(4) $$D > C \text{ oder } D - C > 0$$

die gesuchte Ungleichheit, in welcher nur noch die Veränderlichen w_1, w_2 ... vorkommen.

Ergeben sich jedoch zwei Ungleichheiten mit denselben Ungleichheitszeichen, also entweder $w > C$ und $w > D$ oder

$w < C$ und $w < D$; so kann man keinen Schluss auf die Beziehung zwischen C und D machen, also w nicht eliminiren.

Beispiel 1. Es sei gegeben

$$5 + 6w - 17w_1 > 0$$
$$-9 + 2w + 4w_1 < 0$$

Hieraus folgt durch Auflösung für w

$$w > \frac{-5 + 17w_1}{6} \qquad w < \frac{9 - 4w_1}{2}$$

also

$$\frac{9 - 4w_1}{2} > \frac{-5 + 17w_1}{6}$$

oder wenn man mit 6 multiplizirt und Alles auf Eine Seite stellt

$$32 - 39w_1 > 0$$

Beispiel 2. Wollte man aus den vorstehend gegebenen Ungleichheiten die Veränderliche w_1 eliminiren; so müsste man für w_1 auflösen. Dies gibt

$$w_1 < \frac{5 + 6w}{17} \qquad w_1 < \frac{9 - 2w}{4}$$

Da dies zwei untere Gränzwerthe von w_1 sind; so lassen sie sich nicht kombiniren; es kann also auch w_1 nicht eliminirt werden.

II. Nach dem Prinzipe der Substitution. — Man lös't die Eine der beiden gegebenen Ungleichheiten für w auf, und substituirt den für w gefundenen Gränzwerth statt w in die zweite gegebene Ungleichheit, insofern hierdurch die allgemeine Gültigkeit dieser zweiten Ungleichheit nicht in Frage gestellt wird. Die Substitution muss also unbedingt den Erfolg haben, dass dadurch in der zweiten Ungleichheit die grössere Seite vergrössert oder die kleinere verkleinert wird. Ist Dies nicht unbedingt zu erwarten; so kann die Substitution nicht vorgenommen, also die Elimination von w nicht bewirkt werden.

Um den Erfolg dieser Substitution leicht überblicken zu können, stelle man in der zweiten Ungleichheit die Veränderliche w, welche hier, wo es sich um Ausdrücke vom ersten Grade handelt, nur mit einem bekannten Koeffizienten behaftet sein kann, auf diejenige Seite des Ungleichheitszeichens, wo ihr Koeffizient positiv ist. Hat man alsdann als zweite gegebene Ungleichheit $B > 0$; so kann man darin für w jeden oberen Gränzwerth D setzen, welcher $> w$, oder wofür $w < D$ ist. Hat man dagegen $B < 0$; so kann man darin für w jeden unteren Gränzwerth C setzen, welcher $< w$, oder wofür $w > C$ ist.

Im ersten der beiden obigen Beispiele ergab eine Auflösung der ersten Ungleichheit $w > \frac{-5 + 17w_1}{6}$. Dieser untere Gränz-

werth kann, da in der zweiten gegebenen Ungleichheit $B < 0$ der Koeffizient 2 von w positiv ist, in die letztere substituirt werden. Dies gibt

$$-9+2\left(\frac{-5+17w_1}{6}\right)+4w_1<0$$

also nach Multiplikation mit 3 und gehöriger Reduktion

$$-32+29w_1<0$$

eine Formel, welche mit der vorhin gefundenen $32-29w_1>0$ übereinstimmt.

III. Nach dem Prinzipe der Addition oder Subtraktion. — Durch Multiplikation der gegebenen Ungleichheiten (1) und (2) mit bekannten Zahlen macht man die numerischen Werthe der Koeffizienten von w in beiden gleich (wie bei der Elimination einer Unbekannten zwischen zwei Gleichungen). Erhalten hierdurch diese beiden Koeffizienten entgegengesetzte Zeichen, und sind die Ungleichheitszeichen in (1) und (2) einander gleich; so kann man beide Ungleichheiten addiren, wodurch w verschwindet. Erhalten dagegen jene beiden Koeffizienten gleiche Zeichen, und sind die Ungleichheitszeichen in (1) und (2) entgegengesetzt; so kann man beide Ungleichheiten subtrahiren, wodurch w verschwindet. In allen übrigen Fällen kann die Elimination nicht bewirkt werden.

Multiplizirt man hiernach in dem obigen Beispiele die zweite gegebene Ungleichheit mit 3; so wird dieselbe

$$-27+6w+12w_1<0$$

Hiervon kann die erste gegebene Ungleichheit

$$5+6w-17w_1>0$$

subtrahirt werden. Dies gibt

$$-32+29w_1<0$$

wie vorhin.

Wollte man jedoch w_1 eliminiren, und zu dem Ende die Ungleichheit (1) mit 4 und die Ungleichheit (2) mit 17 multipliziren; so erhielte man zwar die beiden Ungleichheiten

$$20+24w-68w_1>0$$
$$-153+34w+68w_1<0$$

worin die numerischen Werthe von w_1 gleich sind. Dieselben lassen sich jedoch nicht addiren, mithin auch nicht zur Elimination von w_1 gebrauchen.

IV. Man erkennt leicht allgemein, dass sich aus zwei Ungleichheiten von der Form der gegebenen (1) und (2) stets, aber auch nur dann die Veränderliche w eliminiren lässt, wenn bei gleichen Zeichen der Koeffizienten von w die Ungleichheitszeichen in (1) und (2) entgegengesetzt oder wenn bei entgegengesetzten Zeichen jener Koeffizienten diese Ungleichheitszeichen gleich sind.

Es ist übrigens klar, dass aus einem **Paare** von Ungleichheiten wie

$a+pw+qw_1+rw_2+\ldots>\alpha \qquad a+pw+qw_1+rw_2+\ldots<\beta$

obgleich darin die Koeffizienten Ein und derselben Veränderlichen wie w **gleich** und die Ungleichheitszeichen **entgegengesetzt** sind, dennoch eine Elimination von w erfolglos sein würde, weil hierdurch auch alle übrigen Veränderlichen mit verschwinden würden und man die von selbst sich verstehende Beziehung $\beta-\alpha>0$ erhielte.

Wenn jedoch **zwei** derartige Paare, wie

$$(5)\quad \begin{cases} a+pw+qw_1+rw_2+\ldots>\alpha \\ a+pw+qw_1+rw_2+\ldots<\beta \end{cases}$$

$$(6)\quad \begin{cases} a_1+p_1w+q_1w_1+r_1w_2+\ldots>\alpha_1 \\ a_1+p_1w+q_1w_1+r_1w_2+\ldots<\beta_1 \end{cases}$$

gegeben wären; so würden alle zwischen denselben möglichen Eliminationen von w doch nur **zwei** neue Ungleichheiten mit w_1, $w_2\ldots$ ergeben, und diese beiden Ungleichheiten müssen ein **Paar** bilden.

Diese Thatsache sieht man sofort ein, wenn man jede Ungleichheit für w auflös't. Dies gibt

$$(7)\quad w \gtrless \frac{\alpha-a-qw_1-rw_2-\ldots}{p} \qquad w \lessgtr \frac{\beta-a-qw_1-rw_2-\ldots}{p}$$

$$(8)\quad \begin{cases} w \gtrless \dfrac{\alpha_1-a_1-q_1w_1-r_1w_2-\ldots}{p_1} \\ w \lessgtr \dfrac{\beta_1-a_1-q_1w_1-r_1w_2-\ldots}{p_1} \end{cases}$$

In den beiden Ungleichheiten (7) gelten die oberen oder die unteren Ungleichheitszeichen, jenachdem p positiv oder negativ ist, ebenso in den beiden Ungleichheiten (8), jenachdem p_1 positiv oder negativ ist. Immer hat man in (7) und auch in (8) zwei entgegengesetzte Ungleichheitszeichen. Eine Kombination der beiden Ungleichheiten (7) ist aber ebenso fruchtlos, wie eine Kombination der beiden Ungleichheiten (8). Kombinirt man aber eine jede Hälfte des Paares (7) mit der betreffenden Hälfte des Paares (8); so erhält man immer zwei Ungleichheiten, welche, wenn man mit den entstehenden Nennern multiplizirt und gehörig reduzirt, ein **Paar** bilden. Z. B. wenn p und p_1 positiv wären, also in (7) und (8) die oberen Ungleichheitszeichen gälten,

$$(9)\quad \begin{cases} \dfrac{\beta-a-qw_1-rw_2-\ldots}{p} > \dfrac{\alpha_1-a_1-q_1w_1-r_1w_2-\ldots}{p_1} \\ \dfrac{\alpha-a-qw_1-rw_2-\ldots}{p} < \dfrac{\beta_1-a_1-q_1w_1-r_1w_2-\ldots}{p_1} \end{cases}$$

oder nach gehöriger Reduktion

$$(10) \begin{cases}(pa_1-p_1a)+(pq_1-p_1q)w_1+(pr_1-p_1r)w_2+\ldots>p\alpha_1-p_1\beta \\ (pa_1-p_1a)+(pq_1-p_1q)w_1+(pr_1-p_1r)w_2+\ldots<p\beta_1-p_1\alpha\end{cases}$$

§. 48. *Auflösung mehrerer Ungleichheiten mit mehreren Veränderlichen.*

I. Zuvörderst seien zwischen den zwei Veränderlichen w und w_1 folgende r Paare von Ungleichheiten

(1)	$A_1>0$	$B_1<0$
(2)	$A_2>0$	$B_2<0$
(3)	$A_3>0$	$B_3<0$

u. s. w. gegeben. Das allgemeine Prinzip behuf Auflösung dieser Ungleichheiten ist dem bei Auflösung von Gleichungen in Anwendung kommenden ähnlich. Man eliminirt, so oft es angeht, zwischen je zwei der gegebenen Ungleichheiten Eine Veränderliche w. Dies erzeugt, da man (1) mit (2), (1) mit (3) und (2) mit (3) kombiniren kann, im Allgemeinen

$\frac{r(r-1)}{2}$ also bei $r=1$ gegebenen Paaren kein neues Paar
» $r=2$ » » 1 » »
» $r=3$ » » 3 neue Paare
» $r=4$ » » 6 » »
» $r=5$ » » 10 » »

von Ungleichheiten, in welchen nur noch die Veränderliche w_1 vorkommt. Diese Ungleichheiten lös't man für w_1 auf, wodurch sich die Gränzwerthe von w_1 in bekannten Zahlen ergeben. Substituirt man alsdann irgend Einen hiernach für w_1 zulässigen speziellen Werth in die gegebenen Ungleichheiten; so lässt eine Auflösung derselben für w die Gränzen dieser Veränderlichen erkennen, welche jenem Werthe von w_1 entsprechen. Die äussersten Gränzen, welche w bei den verschiedenen Werthen von w_1 zu erreichen fähig ist, ergeben sich, wenn man die für w_1 gefundenen Gränzwerthe so in die gegebenen Ungleichheiten substituirt, dass dieselben unzweifelhaft richtig bleiben, und dieselben alsdann für w auflös't.

Die meiste Bequemlichkeit bei Ausführung dieser Operationen dürfte in der Regel von dem Eliminationsverfahren nach dem Prinzipe der Kombination §. 47, I zu erwarten sein.

Besondere Bemerkungen sind nur für die Fälle zu machen, wo sich w aus den gegebenen Ungleichheiten nicht eliminiren lässt, oder wo sich durch diese Elimination nicht Beziehungen genug zur Bestimmung zweier Gränzen für w_1 ergeben. Alsdann bleibt die Eine Veränderliche entweder ganz, oder doch von einem gewissen Gränzwerthe an willkürlich.

Man kann folgende einzelne Fälle unterscheiden.

II. Eine Ungleichheit mit zwei Veränderlichen. Ist nur die Eine Ungleichheit

$$a+pw+qw_1>0\ ,$$

gegeben; so folgt daraus durch Auflösung für w die einzige Beziehung

$$w \gtrless \frac{-a-qw_1}{p}$$

worin das obere oder untere Zeichen gilt, jenachdem p positiv oder negativ ist. Hierin bleibt w_1 vollkommen willkürlich, und w ist hierdurch für jeden besonderen Werth von w_1 immer nur an Einen Gränzwerth gebunden.

III. Ein Paar von Ungleichheiten mit zwei Veränderlichen. — Ist nur das Eine Paar von Ungleichheiten

$$a+pw+qw_1>0 \qquad b+pw+qw_1<0$$

gegeben; so hat man durch Auflösung für w

$$w \gtrless \frac{-a-qw_1}{p} \qquad w \lessgtr \frac{-b-qw_1}{p}$$

worin die oberen oder die unteren Zeichen gelten, jenachdem p positiv oder negativ ist. Auch hierin bleibt w_1 vollkommen willkürlich; es entsprechen jedoch jedem besonderen Werthe von w_1 zwei Gränzwerthe von w, ein unterer und ein oberer.

IV. Zwei oder mehr Paare von Ungleichheiten mit zwei Veränderlichen. — In diesem Falle ergibt eine Elimination von w mindestens Ein vollständiges Paar von Ungleichheiten mit w_1. Hieraus sind zwei Gränzen für w_1 zu bestimmen, und nach den gegebenen Ungleichheiten entsprechen auch jedem speziellen Werthe von w_1 zwei spezielle Gränzen von w.

Lös't man, um zu diesem Resultate zu gelangen, die gegebenen Ungleichheiten (1), (2), (3) erst für w auf; so werden sich Ausdrücke von der Form

(4) $\qquad w>C_1 \qquad w<D_1$
(5) $\qquad w>C_2 \qquad w<D_2$
(6) $\qquad w>C_3 \qquad w<D_3$

u. s. w. ergeben, durch Kombination hat man hiernach

(7) $\qquad D_1>C_2 \qquad C_1<D_2$
(8) $\qquad D_1>C_3 \qquad C_1<D_3$
(9) $\qquad D_2>C_3 \qquad C_2<D_3$

u. s. w., worin nach §. 47 die einander gegenüber gestellten Ungleichheiten vollständige Paare in Beziehung zu w_1 sein werden.

Lös't man also die letzteren Ungleichheiten für w_1 auf; so kommt

(10) $\qquad w_1>E_1 \qquad w_1<F_1$
(11) $\qquad w_1>E_2 \qquad w_1<F_2$
(12) $\qquad w_1>E_3 \qquad w_1<F_3$

u. s. w. Ist nun E das Maximum von E_1, E_2, E_3 . . . und F das Minimum von F_1, F_2, F_3 . . .; so hat man für w_1 die Auflösung

(13) $$w_1 > E \qquad w_1 < F$$

Wäre $E > F$; so würde die Aufgabe unmöglich sein.

Um nun für einen zwischen E und F liegenden Werth von w_1 die zugehörigen Gränzen für w zu erhalten, substituirt man einen solchen Werth von w_1 in jede der Ungleichheiten (4), (5), (6): ist dann C das Maximum von C_1, C_2, C_3 ... und D das Minimum von D_1, D_2, D_3 ...; so sind die jenem speziellen Werthe von w_1 entsprechenden speziellen Gränzen von w

(14) $$w > C \qquad w < D$$

Wäre $C > D$; so würde es für jenen speziellen Werth von w_1 keinen zugehörigen Werth von w geben.

Wollte man die äussersten Gränzen erkennen, welche w überhaupt zu erreichen vermag, wenn w_1 von E bis F variirt; so müsste man die letzten beiden Gränzwerthe von w_1 dergestalt in die Ungleichheiten (4), (5), (6) substituiren, dass dieselben unbedingt für jeden zulässigen Werth von w richtig bleiben. Ist dann C' das Maximum von C_1, C_2, C_3 ... und D' das Minimum von D_1, D_2, D_3 ...; so hat man

(15) $$w > C' \qquad w < D'$$

Es ist jedoch wohl zu beachten, dass die beiden äussersten Gränzen C' und D' von w nicht j e d e m speziellen Werthe von w_1 zukommen, und überhaupt nicht die z u s a m m e n g e h ö r i g e n Gränzen von w für irgend einen speziellen Werth von w_1 sind.

Wäre $C' > D'$; so würde die ganze Aufgabe unmöglich sein, weil es dann für keinen zulässigen Werth von w_1 zugehörige Werthe von w geben kann. Im Übrigen kann diese Unmöglichkeit in manchen Fällen selbst dann noch vorliegen, wenn auch nicht $C' > D'$ ist, weil C' und D' keine zusammengehörigen Werthe von w sind.

V. M e h r e r e t h e i l s v o l l s t ä n d i g e, t h e i l s u n v o l l s t ä n d i g e P a a r e v o n U n g l e i c h h e i t e n m i t z w e i V e r ä n d e r l i c h e n. — Kommen unter den gegebenen Ungleichheiten unvollständige Paare vor; so ändert der Ausfall der betreffenden Hälften Nichts an den vorstehenden allgemeinen Regeln. Wäre indessen nur E i n vollständiges Paar vorhanden; so kann es sich ereignen, dass die Elimination von w nur Beziehungen hervorbringt, aus welchen sich für w_1 anstatt der Auflösung (13) nur ein einziger Gränzwerth E oder F bestimmen lässt.

Wäre g a r k e i n vollständiges Paar vorhanden; so kann es sich ereignen, dass w_1 nach beiden Seiten willkürlich bleibt.

VI. M e h r e r e U n g l e i c h h e i t e n m i t m e h r e r e n V e r ä n d e r l i c h e n. — Es wird nicht schwer sein, aus dem Vorstehenden das Verfahren zu abstrahiren, welches dann einzuschlagen ist, wenn in der gegebenen Ungleichheit mehr als zwei z. B. die d r e i Veränderlichen w, w_1, w_2 vorkommen.

Man eliminirt erst w, zu welchem Ende man die gegebenen Ungleichheiten (1), (2), (3) in der Form (4), (5), (6) für w auflösen und die Kombinationen (7), (8), (9) bilden kann, welche nur noch w_1 und w_2 enthalten.

Hierauf eliminirt man zwischen den Ungleichheiten (7), (8), (9) die Veränderliche w_1, zu welchem Ende man diese Ungleichheiten in der Form (10), (11), (12) für w_1 auflösen und die Kombinationen

(16) $F_1 > E_2 \qquad E_1 < F_2$
(17) $F_1 > E_3 \qquad E_1 < F_3$
(18) $F_2 > E_3 \qquad E_2 < F_3$

bilden kann, welche nur noch w_2 enthalten.

Lös't man die letzteren Ungleichheiten für w_2 auf; so kommt

(19) $w_2 > G_1 \qquad w_2 < H_1$
(20) $w_2 > G_2 \qquad w_2 < H_2$
(21) $w_2 > G_3 \qquad w_2 < H_3$

und hieraus ergibt sich, wenn G das Maximum von G_1, G_2, G_3 und H das Minimum von H_1, H_2, H_3 ist, als Auflösung für w_2

(22) $w_2 > G \qquad w_2 < H$

Substituirt man irgend einen zwischen G und H liegenden Werth für w_2 in (10), (11), (12); so ergibt sich für das zu jenem speziellen w_2 gehörige w_1

(23) $w_1 > E \qquad w_1 < F$

Substituirt man irgend einen zwischen G und H liegenden Werth für w_2 und irgend einen zwischen E und F liegenden Werth für w_1 in (4), (5), (6); so ergibt sich für das zu jenen speziellen Werthen von w_2 und w_1 gehörige w

(24) $w > C \qquad w < D$

Um die äussersten Gränzen zu überblicken, welche w_1 bei den verschiedenen Werthen von w und welche w_2 bei den verschiedenen Werthen von w und w_1 nicht zu übersteigen vermag; so substituire man die Gränzwerthe G und H von w_2 so in (10), (11), (12), dass diese Ungleichheiten unbedingt für jeden zulässigen Werth von w_1 erfüllt sind. Hierdurch findet man als äusserste Gränzen für w_1

(25) $w_1 > E' \qquad w_1 < F'$

Führt man jetzt sowol die Gränzen C, D für w_2 und die äussersten Gränzen E', F' für w_1 so in (4), (5), (6) ein, dass diese Ungleichheiten unbedingt für alle zulässigen Werthe von w Gültigkeit behalten; so ergibt

(26) $w > C' \qquad w < D'$

die nicht überschreitbaren Gränzen für w.

Wenn die Anzahl der gegebenen vollständigen Paare von Ungleichheiten nicht hinreicht, um für alle Veränderlichen zwei Gränzen zu bestimmen; so wird der Gang der Rechnung jederzeit von selbst die Stelle bezeichnen, wo eine Willkürlichkeit übrig bleibt.

§. 49. Beispiele.

Beispiel 1. Es sei gegeben

(1) $20+3w-4w_1>5 \qquad 20+3w-4w_1<20$

(2) $18-5w+7w_1>15 \qquad 18-5w+7w_1<40$

(3) $-30+2w+3w_1>0 \qquad -30+2w+3w_1<25$

Eine Auflösung für w ergibt

(4) $w>\frac{-15+4w_1}{3} \qquad w<\frac{4w_1}{3}$

(5) $w>\frac{-22+7w_1}{5} \qquad w<\frac{3+7w_1}{5}$

(6) $w>\frac{30-3w_1}{2} \qquad w<\frac{55-3w_1}{2}$

Eine Kombination dieser Ausdrücke gibt

(7) $\frac{4w_1}{3}>\frac{-22+7w_1}{5} \qquad \frac{-15+4w_1}{3}<\frac{3+7w_1}{5}$

(8) $\frac{4w_1}{3}>\frac{30-3w_1}{2} \qquad \frac{-15+4w_1}{3}<\frac{55-3w_1}{2}$

(9) $\frac{3+7w_1}{5}>\frac{30-3w_1}{2} \qquad \frac{-22+7w_1}{5}<\frac{55-3w_1}{2}$

oder wenn man gehörig multiplizirt und reduzirt,

$-w_1>-66 \qquad -w_1<84$

$17w_1>90 \qquad 17w_1<195$

$29w_1>144 \qquad 29w_1<319$

und nun für w_1 auflös't,

(10) $w_1>-84 \qquad w_1<66$

(11) $w_1>5\frac{5}{17} \qquad w_1<11\frac{8}{17}$

(12) $w_1>4\frac{28}{29} \qquad w_1<11$

Hiernach hat man als Auflösung für w_1

(13) $w_1>5\frac{5}{17} \qquad w_1<11$

Hat man es mit einer diophantischen Aufgabe zu thun, in welcher w und w_1 nur ganze Werthe annehmen dürfen; so kann man bei Zulassung der Gränzwerthe

(14) $w_1>6 \qquad w_1<11$

setzen, sodass für w_1 die Zahlen 6, 7, 8, 9, 10, 11 zulässig sind.

Um für irgend einen Werth von w_1, z. B. für $w_1=6$ die Gränzen von w zu finden, so hat man durch Substitution von $w_1=6$ in (4), (5), (6)

(15) $w>3 \qquad w<8$

(16) $w>4 \qquad w<9$

(17) $w>6 \qquad w<18\frac{1}{2}$

also

(18) $w>6 \qquad w<8$

sodass dem Werthe $w_1=6$ die Werthe $w=6$, 7, 8 entsprechen.

Auf diesem Wege erhält man folgende Gesammtheit aller zusammengehörigen Werthe von w_1 und w

$w_1 = 6$	$w = 6, 7, 8$
$= 7$	$= 6, 7, 8, 9$
$= 8$	$= 7, 8, 9, 10$
$= 9$	$= 9, 10, 11, 12$
$= 10$	$= 10, 11, 12$
$= 11$	$= 11$

Wollte man mit Einem Blicke die äussersten Gränzen übersehen, welche w in keinem Falle übersteigen kann; so hat man die Gränzen $5\frac{5}{17}$ und 11 von w_1 aus (13) so in die Ungleichheiten (4), (5), (6) zu substituiren, dass diese Ungleichheiten unzweifelhaft für jeden zulässigen Werth von w gültig bleiben. Demnach ist die untere Gränze $5\frac{5}{17}$ für w_1 in die erste Hälfte der Paare (4), (5) und in die zweite Hälfte des Paares (6), dagegen die obere Gränze 11 für w_1 in die zweite Hälfte der Paare (4), (5) und in die erste Hälfte des Paares (6) zu substituiren. Dies gibt

(19) $\quad w > 2\frac{3}{51} \qquad w < 14\frac{2}{3}$

(20) $\quad w > 3\frac{1}{85} \qquad w < 16$

(21) $\quad w > -1\frac{1}{2} \qquad w < 19\frac{19}{34}$

also

(22) $\quad w > 3\frac{1}{85} \qquad w < 14\frac{2}{3}$

oder in ganzen Zahlen

(23) $\quad w > 3 \qquad w < 14$

Man sieht in der That aus der obigen vollständigen Auflösung, dass diese Gränzen von w nicht überschritten werden.

Beispiel 2. Im dritten Beispiele des §. 35 wurde verlangt, dass

(1) $\quad 655 + 31440y + 1311w > 0 \qquad 655 + 31440y + 1311w < 24$

(2) $\quad 5 + 240y + 10w > 0 \qquad \ldots\ldots$

(3) $\quad y > 0 \qquad \ldots\ldots$

sei. Lös't man diese Ungleichheiten, welche aus Einem vollständigen und zwei unvollständigen Paaren bestehen, für w auf; so kommt

(4) $\quad w > \dfrac{-655 - 31440y}{1311} \qquad w < \dfrac{-631 - 31440y}{1311}$

(5) $\quad w > \dfrac{-1 - 48y}{2} \qquad \ldots\ldots$

Hier ist nur folgende Kombination möglich

(6) $\quad \dfrac{-631 - 31440y}{1311} > \dfrac{-1 - 48y}{2} \qquad \ldots\ldots$

Zu derselben gesellt sich jedoch noch die gegebene Ungleichheit (3), welche nur die Veränderliche y enthält.

Eine Auflösung von (6) gibt, wenn man auch die Ungleichheit (3) darunter schreibt,

(7) $y > -1\frac{1}{48}$ . . . . .

(8) $y > 0$ . . . . .

Die Auflösung für y ist also

(9) $y > 0$

sodass für y alle positiven Zahlen 0, 1, 2, 3 . . . gesetzt werden können. Nimmt man einmal $y = 10$; so muss nach (4) und (5)

$w > -240\frac{415}{1311}$ $w < -240\frac{395}{1311}$

$w > -240\frac{1}{2}$ . . . .

also $w > -240\frac{415}{1311}$ $w < -240\frac{395}{1311}$

sein. Dies würde zwar nicht unmöglich sein, wenn w auch gebrochene Werthe annehmen könnte: da aber in der diophantischen Aufgabe w eine ganze Zahl sein soll; so würde man bei Zulassung der Gränzwerthe haben müssen $w > -240$ $w, < -241$ was entschieden unmöglich ist. Zu dem speziellen Werthe $y = 10$ gibt es also keinen Werth von w.

Nähme man jedoch einmal $y = 81$; so hätte man nach (4) und (5)

$w > -1943\frac{22}{1311}$ $w < -1942\frac{1309}{1311}$

$w > -1944\frac{1}{2}$ . . . . .

also $w > -1943\frac{22}{1311}$ $w < -1942\frac{1309}{1311}$

oder in ganzen Zahlen bei Zulassung der Gränzwerthe $w > -1943$, $w < -1943$. Dieser Bedingung genügt nur der einzige Werth $w = -1943$, sodass man mit $y = 81$ nur $w = -1943$ verbinden kann.

Beispiel 3. Im ersten Beispiele des §. 35 wurde verlangt, dass

(1) $4 + x - 7w > 0$ . . . .

(2) $71 - 20x + 40w > 0$ . . . .

(3) $x > 0$ . . . .

sei. Dies sind drei unvollständige Paare. Lös't man dieselben für w auf; so kommt

(4) . . . . $w < \dfrac{4 + x}{7}$

(5) $w > \dfrac{-71 + 20x}{40}$ . . . .

Hieraus folgt durch Kombination, und wenn man die gegebene Bedingung (3), welche bloss x enthält, darunter schreibt,

(6) $\dfrac{4 + x}{7} > \dfrac{-71 + 20x}{40}$

(7) $x > 0$

und durch Auflösung für x

(8) . . . $x < 6\frac{57}{100}$

(9) $x > 0$ . . .

Die Auflösung für x ist also

(10) $x > 0$ $x < 6\frac{57}{100}$

oder in ganzen Zahlen $x > 0$, $x < 6$, sodass x nur die Werthe 0, 1, 2 . . . 6 haben kann.

Jedem speziellen Werthe von x entspricht aber auch nach (4) und (5) nur eine endliche Reihe Werthe von w. So hat man für $x=3$

(11) $$w > -\frac{11}{40} \qquad w < 1$$

also in ganzen Zahlen $w > 0$, $w < 1$ mithin $w=0$ und 1.

Beispiel 4. Es sei gegeben

(1) $$2+15w+225w_1 > 5 \qquad 2+15w+225w_1 < 7$$

(2) $$5+40w+200w_1 > 10 \qquad 5+40w+200w_1 < 14$$

Hieraus folgt durch Auflösung für w

(3) $$w > \frac{3-225w_1}{15} \qquad w < \frac{5-225w_1}{15}$$

(4) $$w > \frac{5-200w_1}{40} \qquad w < \frac{9-200w_1}{40}$$

mithin durch Kombination

(5) $$\frac{5-225w_1}{15} > \frac{5-200w_1}{40} \qquad \frac{3-225w_1}{15} < \frac{9-200w_1}{40}$$

und durch Auflösung für w_1

(6) $$w_1 > -\frac{3}{1400} \qquad w_1 < \frac{25}{1400}$$

Demnach kann w_1 nur $=0$ sein. Für $w_1=0$ ergeben aber die Ungleichheiten (3) und (4)

(7) $$w > \frac{1}{5} \qquad w < \frac{1}{3}$$

(8) $$w > \frac{1}{8} \qquad w < \frac{9}{40}$$

also (9) $$w > \frac{1}{5} \qquad w < \frac{9}{40}$$

Dies würde zwar für gebrochene Werthe von w, nicht aber für ganze möglich sein. Handelte es sich also um eine diophantische Aufgabe; so wäre dieselbe unmöglich.

Beispiel 5. Man habe für 3 Veränderliche

(1) $$20+3w-4w_1+w_2 > 5 \qquad 20+3w-4w_1+w_2 < 20$$

(2) $$18-5w+7w_1-2w_2 > 15 \qquad 18-5w+7w_1-2w_2 < 40$$

(3) $$w+w_1+w_2 > -9 \qquad w+w_1+w_2 < 9$$

Lös't man für w auf; so kommt

(4) $$w > \frac{-15+4w_1-w_2}{3} \qquad w < \frac{4w_1-w_2}{3}$$

(5) $$w > \frac{-22+7w_1-2w_2}{5} \qquad w < \frac{3+7w_1-2w_2}{5}$$

(6) $$w > -9-w_1-w_2 \qquad w < 9-w_1-w_2$$

Hieraus folgt durch Kombination

$$(7)\quad \begin{cases} \dfrac{4w_1 - w_2}{3} > \dfrac{-22 + 7w_1 - 2w_2}{5} \\ \dfrac{-15 + 4w_1 - w_2}{3} < \dfrac{3 + 7w_1 - 2w_2}{5} \end{cases}$$

$$(8)\quad \begin{cases} \dfrac{4w_1 - w_2}{3} > -9 - w_1 - w_2 \\ \dfrac{-15 + 4w_1 - w_2}{3} < 9 - w_1 - w_2 \end{cases}$$

$$(9)\quad \begin{cases} \dfrac{3 + 7w_1 - 2w_2}{5} > -9 - w_1 - w_2 \\ \dfrac{-22 + 7w_1 - 2w_2}{5} < 9 - w_1 - w_2 \end{cases}$$

und wenn man für w_1 auflös't,

$$(10)\quad w_1 > -84 + w_2 \qquad w_1 < 66 + w_2$$

$$(11)\quad w_1 > \frac{-27 - 2w_2}{7} \qquad w_1 < \frac{42 - 2w_2}{7}$$

$$(12)\quad w_1 > \frac{-48 - 3w_2}{12} \qquad w_1 < \frac{67 - 3w_2}{12}$$

Hieraus folgt durch Kombination

$$(13)\quad 66 + w_2 > \frac{-27 - 2w_2}{7} \qquad -84 + w_2 < \frac{42 - 2w_2}{7}$$

$$(14)\quad 66 + w_2 > \frac{-48 - 3w_2}{12} \qquad -84 + w_2 < \frac{67 - 3w_2}{12}$$

$$(15)\quad \frac{42 - 2w_2}{7} > \frac{-48 - 3w_2}{12} \qquad \frac{-27 - 2w_2}{7} < \frac{67 - 3w_2}{12}$$

und wenn man für w_2 auflös't,

$$(16)\quad w_2 > -54\tfrac{1}{3} \qquad w_2 < 70$$

$$(17)\quad w_2 > -100 \qquad w_2 < 71\tfrac{2}{3}$$

$$(18)\quad w_2 > -264\tfrac{1}{3} \qquad w_2 < 280$$

Die Auflösung für w_2 ist also

$$(19)\quad w_2 > -54\tfrac{1}{3} \qquad w_2 < 70$$

oder in ganzen Zahlen $w_2 > -54$, $w_2 < 70$.

Für den speziellen Werth $w_2 = 10$ erhält man aus (10), (11), (12)

$$w_1 > -74 \qquad w_1 < 76$$

$$w_1 > -6\tfrac{5}{7} \qquad w_1 < 3\tfrac{1}{7}$$

$$w_1 > -6\tfrac{1}{2} \qquad w_1 < 3\tfrac{1}{12}$$

also $w_1 > -6\tfrac{1}{2}$ $\quad w_1 < 3\tfrac{1}{12}$ oder in ganzen Zahlen $w_1 > -6$, $w_1 < 3$, sodass mit $w = 10$ jeder Werth für w_1 von -6 bis 3 verbunden werden kann.

Für die speziellen Werthe $w_2 = 10$, $w_1 = 1$ erhält man aus (4), (5), (6)

$$w > -7 \qquad w < -2$$
$$w > -7 \qquad w < -2$$
$$w > -20 \qquad w < -2$$
also $$w > -7 \qquad w < -2$$
sodass also mit $w = 10$, $w_1 = 1$ die Werthe $w = -7$, -6, -5, -4, -3, -2 verbunden werden können.

Beispiel 6. Es seien im vorstehenden Beispiele zwischen den 3 Veränderlichen w, w_1, w_2 nur die beiden Paare von Ungleichheiten (1), (2) gegeben.

Alsdann erhält man durch Auflösung für w nur die beiden Paare (4), (5), ferner durch Kombination derselben das Paar (7), dessen Auflösung für w_1 zu dem Einen Paare (10) führt.

Hieraus erkennt man, dass die Grösse w_2 vollkommen willkürlich bleibt.

Im Übrigen verfährt man zur Bestimmung der zusammengehörigen speziellen Werthe der Grössen w, w_1, w_2 nach den früheren Prinzipien.

Zweite Auflösungsmethode,

durch Zurückführung der Ungleichheiten auf Gleichungen mit begränzt Veränderlichen.

§. 50. *Vorbereitende Begriffe.*

I. Wenn die von veränderlichen Grössen abhängige, also selbst veränderliche Grösse X an die Bedingung

(1) $$X > a \qquad X < b$$

geknüpft ist; so wollen wir, gemäss dem Früheren, a die untere Gränze oder das Minimum und b die obere Gränze oder das Maximum von X nennen, auch kurz $min X = a$, $max X = b$ schreiben. Es muss nothwendig $b > a$ und demnach $b - a$ durchaus positiv sein, gleichviel ob a oder b selbst positiv oder negativ ist.

Bezeichnet nun φ irgend eine veränderliche Zahl, welche aber positiv ist und zwischen den Gränzen 0 und 1 liegt, und welche wir demnach eine begränzt Veränderliche nennen wollen; so kann man aus dem gegebenen Paare von Ungleichheiten die Gleichung

(2) $$X = a + (b - a)\varphi = min X + (max X - min X)\varphi \ldots (A)$$

bilden, worin $b - a$ und φ entschieden positiv ist, a die untere Gränze von X darstellt, und mit einem Wachsen der Grösse X von a bis b ein Wachsen der Grösse φ von 0 bis 1 verbunden ist. Diese Gleichung wollen wir kurz die Grundform (A) nennen.

Man kann aber auch aus jenem Paare von Ungleichheiten die Gleichung

(3) $X = b - (b-a)\varphi = max\,X - (max\,X - min\,X)\varphi \ldots (B)$
bilden, worin $b-a$ und φ ebenfalls entschieden positiv ist, b die obere Gränze von X darstellt, und mit einem Wachsen der Grösse X von a bis b eine Abnahme der Grösse φ von 1 bis 0 verbunden ist. Diese Gleichung wollen wir die Grundform (B) nennen.

Wenn die Gränzen a und b für sich selbst zulässige Werthe von X sind; so sind die Gränzen 0 und 1 für sich selbst zulässige Werthe von φ.

II. Wäre umgekehrt eine Gleichung von der Grundform (A)

(4) $$X = a + d\varphi$$

gegeben; so findet man die untere Gränze von X für $\varphi = 0$ und die obere für $\varphi = 1$. Mithin ist

$$min\,X = a \qquad max\,X = a + d$$

und daher ist die Gl. (4) gleichbedeutend mit dem Paare von Ungleichheiten

(5) $$X > a \qquad X < a + d$$

Wäre eine Gleichung von der Grundform (B)

(6) $$X = b - d\varphi$$

gegeben; so findet man die untere Gränze von X für $\varphi = 1$ und die obere für $\varphi = 0$. Mithin ist

$$min\;X = b - d \qquad max\;X = b$$

und daher ist die Gl. (6) gleichbedeutend mit dem Paare von Ungleichheiten

(7) $$X > b - d \qquad X < b$$

Hiernach ist es leicht, wenn die Gränzen von X gegeben sind, für X die Gleichung von der Grundform (A) oder (B) herzustellen, und umgekehrt, wenn für X die Gleichung von der Grundform (A) oder (B) gegeben ist, die Gränzen von X zu bestimmen. Man kann also auch leicht von der Form (A) zur Form (B) oder umgekehrt übergehen.

III. Auch der Fall, wo die Grösse X konstant ist, lässt sich dem vorstehenden unterordnen. Es sind hierfür die beiden Gränzen von X gleich, also $a = b$ oder $min\;X = max\;X$, mithin $d = b - a = 0$, folglich für beide Grundformen $X = a$.

Wäre für X nur Eine Gränze gegeben, also X nach der andern Seite unbegränzt; so sei U das Zeichen für eine positive Zahl, welche jedes Maass der Grösse übersteigt. Ist alsdann für X die untere Gränze a gegeben; so kann man U für die obere Gränze annehmen, und demnach $min\;X = a$, $max\;X = U$, also $d = U - a$ und nach der Grundform (A)

(8) $$X = a + (U - a)\varphi$$

setzen. Ist jedoch für X die obere Gränze b gegeben; so kann man $-U$ für die untere Gränze annehmen, und demnach $min\;X = -U$, $max\;X = b$, also $d = b - (-U) = U + b$ und nach der Grundform (A)

(9) $$X = -U + (U + b)\varphi$$
setzen.

Wäre für X gar keine Gränze gegeben, bliebe also diese Grösse nach beiden Seiten unbegränzt; so kann man *min* $X = -U$, *max* $X = U$, also $d = U - (-U) = 2U$ und nach der Grundform (A)

(10) $$X = -U + 2U\varphi$$
setzen.

IV. Betrachten wir jetzt Ausdrücke von beliebiger Zusammensetzung, in welchen derartige begränzt veränderliche Grössen wie φ vorkommen. Die Werthe solcher Ausdrücke werden nach der Natur der darin verflochtenen Grössen im Allgemeinen zwischen einer unteren und einer oberen Gränze variiren. Dieselben werden also auf jede der obigen beiden Grundformen gebracht werden können. Hätte man z. B.

$$X = \frac{5}{2 + 7\varphi}$$

so ist klar, dass X sein Minimum für $\varphi = 1$ und sein Maximum für $\varphi = 0$ erreicht, dass also *min* $X = \frac{5}{9}$ und *max* $X = \frac{5}{2}$, folglich nach der Grundform (A)

$$X = \frac{5}{9} + \left(\frac{5}{2} - \frac{5}{9}\right)\varphi_1 = \frac{5}{9} + \frac{35}{18}\varphi_1$$

ist, worin φ_1 eine von 0 bis 1 veränderliche Grösse wie φ darstellt.

Es können auch mehrere von einander ganz unabhängige begränzt Veränderliche φ, ψ, χ ... von der obigen Beschaffenheit in einer Formel vorkommen. Wäre z. B.

$$X = 3 + 4\varphi - 6\psi + 2\chi$$

so ergibt sich offenbar das Minimum von X für $\varphi = 0$, $\chi = 0$, $\psi = 1$ und das Maximum für $\varphi = 1$, $\chi = 1$, $\psi = 0$. Man hat also *min* $X = -3$, *max* $X = 9$, folglich

$$X = -3 + [9 - (-3)]\varphi_1 = -3 + 12\varphi_1$$

Diese Verwandlungen sind besonders dann von Wichtigkeit, wenn die Rechnung mit den Grundformen zu Ausdrücken führt, welche jenen Formen nicht mehr entsprechen. Man wird dann das Endresultat auf eine Grundform zurückzuführen suchen, weil hierin die Beziehungen am anschaulichsten hervortreten. Der Übung wegen sind die folgenden Paragraphen den aus den einfachsten Rechnungsoperationen hervorgehenden Formverwandlungen gewidmet. Wir setzen dabei voraus, dass die gegebenen Ausdrücke sämmtlich die Grundform (A) haben, und stellen das Resultat der Rechnung wiederum in diese Form.

§. 51. ***Addition der Grundformen mit begränzt Veränderlichen.***

In den nächstfolgenden Paragraphen werden wir die einfachsten Rechnungsverknüpfungen der beiden Ausdrücke

(1) $$X = a + d\,\varphi$$

(2) $$X_1 = a_1 + d_1\,\varphi_1$$

und einer konstanten Zahl c (welche übrigens auch als spezieller Fall Eines dieser Ausdrücke als $c + 0\varphi$ gedacht werden kann) näher betrachten.

Für die Addition hat man zuvörderst

(3) $$X + c = a + c + d\varphi$$

Diese Gleichung entspricht schon der Grundform (A); man hat für

$$\varphi = 0 \text{ das } min\ (X + c) = a + c$$
$$\varphi = 1 \text{ das } max\ (X + c) = a + c + d$$

Ferner ist $X + X_1 = a + a_1 + d\varphi + d_1\varphi_1$, also für

$$\varphi = 0, \varphi_1 = 0 \text{ das } min\ (X + X_1) = a + a_1$$
$$\varphi = 1, \varphi_1 = 1 \text{ das } max\ (X + X_1) = a + a_1 + d + d_1, \text{ mithin}$$

(4) $$X + X_1 = a + a_1 + (d + d_1)\,\psi$$

§. 52. ***Subtraktion der Grundformen mit begränzt Veränderlichen.***

Man hat sofort in gewünschter Form

(1) $$X - c = a - c + d\varphi$$

Ferner ist $X - X_1 = a - a_1 + d\varphi - d_1\varphi_1$, also für

$$\varphi = 0,\ \varphi_1 = 1 \text{ das } min\ (X - X_1) = a - a_1 - d_1$$
$$\varphi = 1,\ \varphi_1 = 0 \text{ das } max\ (X - X_1) = a - a_1 + d, \text{ mithin}$$

(2) $$X - X_1 = a - a_1 - d_1 + (d + d_1)\,\psi$$

§. 53. ***Multiplikation der Grundformen mit begränzt Veränderlichen.***

I. Man hat sofort, wenn c positiv ist, in gewünschter Form

(1) $$cX = ac + cd\varphi$$

Wenn jedoch der konstante Faktor negativ ist; so wollen wir $-c$ dafür nehmen.

Alsdann ist $-cX = -ac - cd\varphi$, also für

$$\varphi = 1 \text{ das } min\ (-cX) = -ac - cd$$
$$\varphi = 0 \text{ das } max\ (-cX) = -ac, \text{ mithin}$$

(2) $$-cX = -(a + d)c + cd\varphi$$

Was die Reduktion des Produktes

$$XX_1 = aa_1 + a_1 d\varphi + ad_1\varphi_1 + dd_1\,\varphi\varphi_1$$

betrifft; so hat man folgende drei Fälle zu unterscheiden.

II. Erster Fall. a und a_1 sind beide positiv. Alsdann hat man offenbar für

$$\varphi = 0,\ \varphi_1 = 0 \text{ das } min\ (XX_1) = aa_1$$
$$\varphi = 1,\ \varphi_1 = 1 \text{ das } max\ (XX_1) = aa_1 + a_1 d + ad_1 + dd_1$$
$$= (a + a_1)\,(d + d_1)$$

mithin

(3) $$XX_1 = aa_1 + [(a + a_1)(d + d_1) - aa_1]\psi$$

III. **Zweiter Fall.** a ist positiv und a_1 negativ. In diesem und dem folgenden Falle ist es rathsam, das Produkt XX_1 in die Form

$$XX_1 = (a + d\varphi)(a_1 + d_1\varphi_1) = dd_1\left(\frac{a}{d} + \varphi\right)\left(\frac{a_1}{d_1} + \varphi_1\right)$$

zu bringen. Da a_1 negativ sein soll; so schreiben wir zu grösserer Deutlichkeit

$$XX_1 = (a + d\varphi)(-a_1 + d_1\varphi_1) = -dd_1\left(\frac{a}{d} + \varphi\right)\left(\frac{a_1}{d_1} - \varphi_1\right)$$

Ist nun $a_1 > d_1$, also $\frac{a_1}{d_1} > 1$; so ist $\frac{a_1}{d_1} - \varphi_1$ stets positiv, also XX_1 stets negativ, und man hat für

$\varphi = 1, \varphi_1 = 0$ das *min* $(XX_1) = -a_1(a + d) = -aa_1 - a_1 d$

$\varphi = 0, \varphi_1 = 1$ das *max* $(XX_1) = -a(a_1 - d_1) = -aa_1 + ad_1$

mithin

(4) $$XX_1 = -a_1(a + d) + (ad_1 + a_1 d)\psi$$

Ist dagegen $a_1 < d_1$, also $\frac{a_1}{d_1} < 1$; so kann für geeignete Werthe von φ_1 die Grösse $\frac{a_1}{d_1} - \varphi_1$ sowol positiv, wie negativ werden. Das Minimum von XX_1 entspricht also dem negativen Werthe dieses Produkts von möglichst grossem absoluten Betrage, und das Maximum von XX_1 entspricht dem positiven Werthe dieses Produkts von möglichst grossem Betrage. Man hat also für

$\varphi = 1, \varphi_1 = 0$ das *min* $(XX_1) = -a_1(a + d) = -aa_1 - a_1 d$

$\varphi = 1, \varphi_1 = 1$ das *max* $(XX_1) = (a + d)(-a_1 + d_1) =$
$-aa_1 + ad_1 - a_1 d + dd_1$, mithin

(5) $$XX_1 = -a_1(a + d) + d_1(a + d)\psi$$

Ist $a_1 = d_1$ also $\frac{a_1}{d_1} = 1$; so kann man sich sowol der Formel (4), wie auch der Formel (5) bedienen.

IV. **Dritter Fall.** a und a_1 sind beide negativ. Zu grösserer Deutlichkeit schreiben wir

$$XX_1 = (-a + d\varphi)(-a_1 + d_1\varphi_1) = dd_1\left(\frac{a}{d} - \varphi\right)\left(\frac{a_1}{d_1} - \varphi_1\right)$$

Ist $a > d$, $a_1 > d_1$, also $\frac{a}{d} > 1, \frac{a_1}{d_1} > 1$; so ist $\frac{a}{d} - \varphi$ und $\frac{a_1}{d_1} - \varphi_1$ stets positiv und man hat für

$\varphi = 1, \varphi_1 = 1$ das *min* $(XX_1) = (a - d)(a_1 - d_1)$

$\varphi = 0, \varphi_1 = 0$ das *max* $(XX_1) = aa_1$, mithin

(6) $XX_1 = (a-d)(a_1-d_1) + [aa_1 - (a-d)(a_1-d_1)]\psi$

Ist $a > d$, $a_1 < d_1$, also $\frac{a}{d} > 1$, $\frac{a_1}{d_1} < 1$; so ist $\frac{a}{d} - \varphi$ stets positiv, jedoch $\frac{a_1}{d_1} - \varphi_1$ kann sowol positiv, wie negativ werden. Demnach hat man für

$$\varphi = 0,\ \varphi_1 = 1 \text{ das } min\ (XX_1) = a(a_1 - d_1)$$
$$\varphi = 0,\ \varphi_1 = 0 \text{ das } max\ (XX_1) = aa_1, \text{ mithin}$$

(7) $$XX_1 = a(a_1 - d_1) + ad_1\psi$$

Ist $a < d$, $a_1 < d_1$, also $\frac{a}{d} < 1$, $\frac{a_1}{d_1} < 1$; so kann jede der Grössen $\frac{a}{d} - \varphi$ und $\frac{a_1}{d_1} - \varphi_1$ sowol positiv, wie negativ werden. Das Minimum von XX_1 ist also negativ und entspricht dem negativen Werthe von XX_1 vom grösstmöglichen numerischen Betrage. Dieses Minimum wird entweder in der Form $-dd_1\left(\frac{a}{d} - \varphi\right)\left(\varphi_1 - \frac{a_1}{d_1}\right)$ oder in der Form $-dd_1\left(\varphi - \frac{a}{d}\right)\left(\frac{a_1}{d_1} - \varphi_1\right)$ enthalten sind, worin die in Klammern geschlossenen Ausdrücke positiv sind, und es kommt zur Bestimmung desselben nur darauf an, ob $\left(\frac{a}{d} - \varphi\right)\left(\varphi_1 - \frac{a_1}{d_1}\right)$ oder $\left(\varphi - \frac{a}{d}\right)\left(\frac{a_1}{d_1} - \varphi_1\right)$ den grösseren Betrag annehmen kann. Offenbar muss, wenn die erstere Form gelten sollte, $\varphi = 0$, $\varphi_1 = 1$, und wenn die letztere Form gelten sollte, $\varphi = 1$, $\varphi_1 = 0$ gesetzt werden. Hiernach ist leicht zu sehen, dass

$$\text{wenn } \frac{a}{d} > \frac{a_1}{d_1} \text{ ist, sich für}$$
$$\varphi = 0,\ \varphi_1 = 1 \text{ das } min\ (XX_1) = -a(d_1 - a_1)$$
$$\text{und wenn } \frac{a}{d} < \frac{a_1}{d_1} \text{ ist, sich für}$$
$$\varphi = 1,\ \varphi_1 = 0 \text{ das } min\ (XX_1) = -a_1(d - a)$$

ergibt.

Das Maximum von XX_1 ist positiv und entspricht dem positiven Werthe von XX_1 vom grösstmöglichen numerischen Betrage. Dieses Maximum wird also entweder in der Form

$$dd_1\left(\frac{a}{d} - \varphi\right)\left(\frac{a_1}{d_1} - \varphi_1\right) \text{ oder in der Form}$$
$$dd_1\left(\varphi - \frac{a}{d}\right)\left(\varphi_1 - \frac{a_1}{d_1}\right)$$

enthalten sein, worin die in Klammern geschlossenen Ausdrücke

positiv sind. Offenbar muss, wenn die erstere Form gelten sollte, $\varphi = 0$, $\varphi_1 = 0$ und wenn die letztere Form gelten sollte, $\varphi = 1$, $\varphi_1 = 1$ gesetzt werden. Hiernach erkennt man leicht, dass

wenn $\frac{a}{d} + \frac{a_1}{d_1} > 1$ ist, sich für

$\varphi = 0$, $\varphi_1 = 0$ das $max\ (XX_1) = aa_1$

und wenn $\frac{a}{d} + \frac{a_1}{d_1} < 1$ ist, sich für

$\varphi = 1$, $\varphi_1 = 1$ das $max\ (XX_1) = (a - d)\ (a - d_1)$

ergibt.

Hiernach wird es je nach den besonderen Umständen stets leicht sein, den Werth von XX_1 in der Form

$min\ (XX_1) + [max\ (XX_1) - min\ (XX_1)]\ \psi$ darzustellen.

Wenn die im vorstehenden dritten Falle spezifizirten Bedingungen nicht ganz streng erfüllt sind, man vielmehr an irgend einer Stelle statt des Zeichens $>$ oder $<$ das Zeichen $=$ hat; so kann man sich ebensowol der für $>$, als auch der für $<$ aufgestellten Formel bedienen.

§. 54. *Division der Grundformen mit begränzt Veränderlichen.*

I. Man hat sofort wiederum in Grundform, wenn c positiv ist,

(1) $$\frac{X}{c} = \frac{a}{c} + \frac{d}{c}\varphi$$

Wenn jedoch c negativ ist, und wir zu grösserer Deutlichkeit $-c$ dafür schreiben; so ist $\frac{X}{-c} = -\frac{a}{c} - \frac{d}{c}\varphi$; man hat also für

$$\varphi = 1 \text{ das } min\left(\frac{X}{-c}\right) = -\frac{a+d}{c}$$

$$\varphi = 0 \text{ das } max\left(\frac{X}{-c}\right) = -\frac{a}{c} \text{ mithin}$$

(2) $$\frac{X}{-c} = -\frac{a+d}{c} + \frac{d}{c}\varphi$$

Was die Reduktion des Quotienten

$$\frac{X}{X_1} = \frac{a + d\varphi}{a_1 + d_1\varphi_1} = \frac{d}{d_1} \cdot \frac{\frac{a}{d} + \varphi}{\frac{a_1}{d_1} + \varphi_1}$$

betrifft; so unterscheiden wir folgende vier Fälle.

II. **Erster Fall. a und a_1 sind beide positiv.** Alsdann hat man für

$$\varphi = 0,\ \varphi_1 = 1 \text{ das } min \left(\frac{X}{X_1}\right) = \frac{a}{a_1 + d_1}$$

$$\varphi = 1,\ \varphi_1 = 0 \text{ das } max \left(\frac{X}{X_1}\right) = \frac{a+d}{a_1} \quad \text{mithin}$$

(3) $$\frac{X}{X_1} = \frac{a}{a_1 + d_1} + \frac{(a+d)\,(a_1+d_1) - aa_1}{a_1\,(a_1+d_1)}\,\psi$$

III. Zweiter Fall. a ist positiv und a_1 negativ. Zu grösserer Deutlichkeit schreiben wir jetzt

$$\frac{X}{X_1} = \frac{a + d\,\varphi}{-a_1 + d_1\,\varphi_1} = -\frac{d}{d_1}\cdot\frac{\frac{a}{d} + \varphi}{\frac{a_1}{d_1} - \varphi_1}$$

Ist $a_1 > d_1$, also $\frac{a_1}{d_1} > 1$; so ist $\frac{a_1}{d_1} - \varphi_1$ stets positiv, also $\frac{X}{X_1}$ stets negativ; man hat also für

$$\varphi = 1,\ \varphi_1 = 1 \text{ das } min \left(\frac{X}{X_1}\right) = -\frac{a+d}{a_1 - d_1}$$

$$\varphi = 0,\ \varphi_1 = 0 \text{ das } max \left(\frac{X}{X_1}\right) = -\frac{a}{a_1}, \text{ mithin}$$

(4) $$\frac{X}{X_1} = -\frac{a+d}{a_1 - d_1} + \frac{a_1\,(a+d) - a\,(a_1 - d_1)}{a_1\,(a_1 - d_1)}\,\psi$$

Ist $a_1 < d_1$, also $\frac{a_1}{d_1} < 1$; so kann $\frac{a_1}{d_1} - \varphi_1$ sowol positiv, wie negativ, natürlich auch $= 0$ werden. Man hat jetzt offenbar für

$$\varphi = 1,\ \varphi_1 = \frac{a_1}{d_1} \text{ das } min \left(\frac{X}{X_1}\right) = -\frac{a+d}{0} = -U$$

Das Maximum, welches positiv und demnach in der Form $\frac{d}{d_1}\cdot\frac{\frac{a}{d} + \varphi}{\varphi_1 - \frac{a_1}{d_1}}$ enthalten ist, entspricht offenbar denselben Werthen von φ und φ_1 wie das Minimum. Man hat also für

$$\varphi = 1,\ \varphi_1 = \frac{a_1}{d_1} \text{ das } max \left(\frac{X}{X_1}\right) = \frac{a+d}{0} = +U, \text{ mithin}$$

(5) $$\frac{X}{X_1} = -U + 2\,U\psi$$

Ist $a_1 = d_1$, also $\frac{a_1}{d_1} = 1$; so gilt die Formel (5).

IV. Dritter Fall, a ist negativ und a_1 positiv. Wir setzen jetzt

$$\frac{X}{X_1} = \frac{-a+d\varphi}{a_1+d_1\varphi_1} = -\frac{d}{d_1}\cdot\frac{\frac{a}{d}-\varphi}{\frac{a_1}{d_1}+\varphi_1}$$

Ist $a > d$, also $\frac{a}{d} > 1$; so ist $\frac{a}{d} - \varphi$ stets positiv, also $\frac{X}{X_1}$ stets negativ. Man hat daher für

$\varphi = 0, \varphi_1 = 0$ das *min* $\left(\frac{X}{X_1}\right) = -\frac{a}{a_1}$

$\varphi = 1, \varphi_1 = 1$ das *max* $\left(\frac{X}{X_1}\right) = -\frac{a-d}{a_1-d_1}$, mithin

(6) $$\frac{X}{X_1} = -\frac{a}{a_1} + \frac{a(a_1-d_1) - a_1(a-d)}{a_1(a_1-d_1)}\psi$$

Ist $a < d$, also $\frac{a}{d} < 1$; so kann $\frac{a}{d} - \varphi$ sowol positiv, wie negativ werden. Man hat jetzt für

$\varphi = 0, \varphi_1 = 0$ das *min* $\left(\frac{X}{X_1}\right) = -\frac{a}{a_1}$

$\varphi = 1, \varphi_1 = 0$ das *max* $\left(\frac{X}{X_1}\right) = \frac{d-a}{a_1}$, mithin

(7) $$\frac{X}{X_1} = -\frac{a}{a_1} + \frac{d}{a_1}\psi$$

Ist $a = d$, also $\frac{a}{d} = 1$; so kann man sich sowol der Formel (6), wie auch der Formel (7) bedienen.

V. Vierter Fall. a und a_1 sind beide negativ. Wir setzen jetzt

$$\frac{X}{X_1} = \frac{-a+d\varphi}{-a_1+d_1\varphi_1} = \frac{d}{d_1}\cdot\frac{\frac{a}{d}-\varphi}{\frac{a_1}{d_1}-\varphi_1}$$

Ist $a \geqq d$, $a_1 \geqq d_1$ also $\frac{a}{d} \geqq 1$, $\frac{a_1}{d_1} \geqq 1$; so sind die beiden Grössen $\frac{a}{d} - \varphi$ und $\frac{a_1}{d_1} - \varphi_1$ stets positiv, und die letztere kann nicht $= 0$ werden.

Man hat demnach für

$\varphi = 1, \varphi_1 = 0$ das *min* $\left(\frac{X}{X_1}\right) = \frac{a-d}{a_1}$

$\varphi = 0, \varphi_1 = 1$ das *max* $\left(\frac{X}{X_1}\right) = \frac{a}{a_1-d_1}$, mithin

(8) $$\frac{X}{X_1} = \frac{a-d}{a_1} + \frac{aa_1 - (a-d)\,(a_1 - d_1)}{a_1(a_1 - d_1)}\,\psi$$

Ist $a \leqq d$, $a_1 > d_1$, also $\frac{a}{d} \leqq 1$, $\frac{a_1}{d_1} > 1$; so ist der Nenner $\frac{a_1}{d_1} - \varphi_1$ stets positiv; der Zähler $\frac{a}{d} - \varphi$ kann aber positiv und negativ werden. Man hat also für

$$\varphi = 1,\ \varphi_1 = 1 \text{ das } \min\left(\frac{X}{X_1}\right) = -\frac{d-a}{a_1 - d_1}$$

$$\varphi = 0,\ \varphi_1 = 1 \text{ das } \max\left(\frac{X}{X_1}\right) = \frac{a}{a_1 - d_1} \text{ mithin}$$

(9) $$\frac{X}{X_1} = -\frac{d-a}{a_1 - d_1} + \frac{d}{a_1 - d_1}\,\psi$$

Ist $a \geqq d$, $a_1 \leqq d_1$, also $\frac{a}{d} \geqq 1$, $\frac{a_1}{d_1} \leqq 1$; so ist der Zähler $\frac{a}{d} - \varphi$ stets positiv; der Nenner $\frac{a_1}{d_1} - \varphi$ kann aber positiv und negativ, auch $= 0$ werden. Man hat dann das negative Minimum aus der Form $-\frac{d}{d_1} \cdot \frac{\frac{a}{d} - \varphi}{\varphi_1 - \frac{a_1}{d_1}}$ zu bestimmen. Dies gibt für

$$\varphi = 0,\ \varphi_1 = \frac{a_1}{d_1} \text{ das } \min\left(\frac{X}{X_1}\right) = -\frac{a}{0} = -U$$

Das positive Maximum hat man aus der Form $\frac{d}{d_1} \cdot \frac{\frac{a}{d} - \varphi}{\frac{a_1}{d_1} - \varphi_1}$ zu bestimmen. Dies gibt für

$$\varphi = 0,\ \varphi_1 = \frac{a_1}{d_1} \text{ das } \max\left(\frac{X}{X_1}\right) = \frac{a}{0} = +U, \text{ mithin}$$

(10) $$\frac{X}{X_1} = -U + 2U\psi$$

Ist $a \leqq d$, $a_1 \leqq d_1$, also $\frac{a}{d} \leqq 1$, $\frac{a_1}{d_1} \leqq 1$; so kann sowol der Zähler $\frac{a}{d} - \varphi$, wie auch der Nenner $\frac{a_1}{d_1} - \varphi_1$ positiv und negativ werden. Das Minimum ist alsdann negativ $= -U$ und das Maximum positiv $= +U$, also

(11) $$\frac{X}{X_1} = -U + 2U\psi.$$

§. 55. *Anwendung der Gleichungen mit begränzt Veränderlichen auf die Bestimmung der Gränzen für die Willkürlichen der unbestimmten Gleichungen.*

Wendet man die in den letzten Paragraphen erörterten Formen mit begränzt Veränderlichen auf die Bestimmung der Willkürlichen an, welche in den Auflösungen der unbestimmten Gleichungen erscheinen; so hat man es im Laufe der Rechnung nur mit Gleichungen und nicht mit Ungleichheiten zu thun, was in mancher Hinsicht Bequemlichkeit, besonders aber eine grössere Ökonomie der Formeln gewährt.

Wenn man beachtet, dass durch die in Rede stehenden neuen Formen eine Grösse nicht fest bestimmt, sondern nur zwischen gewisse Gränzen eingeschlossen ist; so wird es nicht befremden, dass hinundwieder mehr Gleichungen, als unbekannte und gesuchte Grössen gegeben sind. Die begränzt Veränderlichen φ, ψ... sind bei diesen Rechnungen nicht einmal zu den unbekannten und gesuchten Grössen zu zählen; dieselben sind vielmehr wie unbestimmte bekannte Grössen anzusehen, welche einen willkürlichen Werth von 0 bis 1 annehmen können.

Hätte man etwa

(1) $x = 10 + 7\varphi$

(2) $x = 9 + 3\varphi_1$

so folgt aus (1) $\quad min\ x = 10,\quad max\ x = 17$

aus (2) $\quad min\ x = 9,\quad max\ x = 12$

also aus (1) und (2) $\quad min\ x = 9,\quad max\ x = 17$

Folglich ist, wenn die beiden Gleichungen (1) und (2) zusammen bestehen sollen

(3) $x = 9 + 8\psi$

Es ist klar, dass man in einem Systeme von mehreren solchen gegebenen Gleichungen jede zwei als selbstständige zu behandeln und miteinander zu kombiniren hat, indem, wenn z. B. drei Gleichungen gegeben wären, die Erfüllung der ersten und zweiten und die Erfüllung der ersten und dritten keineswegs die Erfüllung der zweiten und dritten nothwendig bedingt.

Die sonstigen Eigenthümlichkeiten der Rechnung, welche den bei den Ungleichheiten vorkommenden analog sind, werden am besten aus einigen Beispielen erhellen, wozu wir zunächst mehrere der bereits in §. 49 mittelst Ungleichheiten gelös'ten Aufgaben wählen.

Beispiel 1. Nach dem ersten Beispiele des §. 49 soll $20 + 3w - 4w_1 > 5$ und < 20, also $= 5 + (20 - 5)\varphi_1 = 5 + 15\varphi_1$, ferner soll $18 - 5w + 7w_1 > 15$ und < 40, also $= 15 + (40 - 15)\varphi_2 = 15 + 25\varphi_2$, endlich $-30 + 2w + 3w_1 > 0$ und < 25, also $= 0 + (25 - 0)\varphi_3 = 0 + 25\varphi_3$ sein. Es sind also folgende drei Gleichungen mit den beiden Unbekannten w, w_1 gegeben:

$$(1)\quad 20+3w-4w_1 = 5+15\varphi_1$$
$$(2)\quad 18-5w+7w_1 = 15+25\varphi_2$$
$$(3)\quad -30+2w+3w_1 = 25\varphi_3$$

Lös't man jede dieser Gleichungen für w auf; so kommt

$$(4)\quad w = \frac{4w_1-15+15\varphi_1}{3}$$

$$(5)\quad w = \frac{7w_1+3-25\varphi_2}{5}$$

$$(6)\quad w = \frac{-3w_1+30+25\varphi_3}{2}$$

Setzt man je zwei dieser Werthe von w einander gleich, und lös't jede hierdurch sich ergebende Gleichung für w_1 auf; so kommt

$$(7)\quad w_1 = -84+75\varphi_1+75\varphi_2$$

$$(8)\quad w_1 = \frac{120-30\varphi_1+75\varphi_3}{17}$$

$$(9)\quad w_2 = \frac{144+50\varphi_2+125\varphi_3}{29}$$

Nun folgt, jenachdem man w_1 aus Gl. (7) oder aus (8) oder aus (9) gegeben denkt,

aus (7) für $\varphi_1=0$, $\varphi_2=0$ das $min\ w_1 = -84$
für $\varphi_1=1$, $\varphi_2=0$ das $max\ w_1 = 66$

aus (8) für $\varphi_1=1$, $\varphi_3=0$ das $min\ w_1 = \frac{90}{17} = 5\frac{5}{17}$

für $\varphi_1=0$, $\varphi_3=1$ das $max\ w_1 = \frac{195}{17} = 11\frac{8}{17}$

aus (9) für $\varphi_2=0$, $\varphi_3=0$ das $min\ w_1 = \frac{144}{29} = 4\frac{28}{29}$

für $\varphi_2=1$, $\varphi_3=1$ das $max\ w_1 = \frac{319}{29} = 11$

Hieraus ergibt sich als gesuchte Auflösung für w_1

$min\ w_1 = 5\frac{5}{17}$ $\qquad$ $max\ w_1 = 11$ oder

$$(10)\quad w_1 = \frac{90}{17}+\frac{97}{17}\psi$$

Diese Auflösung stimmt mit der in §. 49 in der Form $w_1 > 5\frac{5}{17}$, $w_1 < 11$ gefundenen genau überein.

Um für einen speziellen Werth von w_1, z. B. für $w_1 = 6$ die zugehörigen Gränzen von w zu finden, hat man diesen Werth in die Gleichungen (4), (5), (6) zu substituiren. Dies gibt

(11) $w = 3 + 5\varphi_1$

(12) $w = 9 - 5\varphi_2$

(13) $w = \frac{12 + 25\varphi_3}{2}$

Demnach hat man

aus (11) für $\varphi_1 = 0$ das *min* $w = 3$

für $\varphi_1 = 1$ das *max* $w = 8$

aus (12) für $\varphi_2 = 1$ das *min* $w = 4$

für $\varphi_2 = 0$ das *max* $w = 9$

aus (13) für $\varphi_3 = 0$ das *min* $w = 6$

für $\varphi_3 = 1$ das *max* $w = \frac{37}{2} = 18\frac{1}{2}$

Hieraus ergibt sich

min $w = 6$ *max* $w = 8$

Die zu $w_1 = 6$ gehörigen Werthe von w sind also 6, 7, 8, wie auch in §. 49 gefunden ist.

Was die unmöglichen Fälle betrifft; so liegen dieselben offenbar da vor, wo für dieselbe Grösse mehrere Minima und mehrere Maxima in Betracht kommen, und das grösste Minimum grösser ist, als das kleinste Maximum.

Beispiel 2. Die 3 Paar Ungleichheiten mit den 3 Unbekannten w, w_1, w_2 in dem Beispiele 5 des §. 49 sind gleichbedeutend mit folgenden 3 Gleichungen:

(1) $20 + 3w - 4w_1 + w_2 = 5 + 15\varphi_1$

(2) $18 - 5w + 7w_1 - 2w_2 = 15 + 25\varphi_2$

(3) $w + w_1 + w_2 = -9 + 18\varphi_3$

Eine Auflösung für w ergibt

(4) $w = \frac{4w_1 - w_2 - 15 + 15\varphi_1}{3}$

(5) $w = \frac{7w_1 - 2w_2 + 3 - 25\varphi_2}{5}$

(6) $w = -w_1 - w_2 - 9 + 18\varphi_3$

Setzt man je zwei dieser Ausdrücke von w einander gleich, und lös't jede entstehende Gleichung für w_1 auf; so kommt

(7) $w_1 = w_2 - 84 + 75\varphi_1 + 75w_2$

(8) $w_1 = \frac{-2w_2 - 12 - 15\varphi_1 + 54\varphi_3}{7}$

(9) $w_1 = \frac{-3w_2 - 48 + 25\varphi_2 + 90\varphi_3}{12}$

Setzt man je zwei dieser Ausdrücke von w_1 einander gleich, und lös't jede sich ergebende Gleichung für w_2 auf; so erhält man Ein und denselben Werth für w_2, nämlich

(10) $w_2 = \frac{192 - 180\varphi_1 - 175\varphi_2 + 18\varphi_3}{3}$

Dass sich aus der Kombination der drei Gleichungen (7), (8), (9) nur ein einziger Werth für w_2 ergeben kann, leuchtet schon daraus ein, dass ursprünglich zwischen drei Unbekannten w, w_1, w_2 3 Gleichungen gegeben sind. In einem solchen Falle vereinfacht sich also die Rechnung gegen die mit Ungleichheiten in einem noch höheren Grade, indem sich die in §. 49 nothwendig gewesene Betrachtung noch anderer Ausdrücke von w_2 als überflüssig erweis't. Derartige Ausscheidungen überflüssiger Formeln sind offenbar bei der Methode des §. 49 ganz unthunlich, weil dort nicht die Wirkung einer Grösse wie φ_1, φ_2 oder φ_3, die allerdings willkürlich ist, aber doch immer nur von einem einzigen gewissen Werthe sein kann, sich nicht bis ans Ende der Rechnung ermessen lässt, und das dortige Verfahren bei der jetzigen Methode seine Analogie darin finden würde, dass man in jeder während der Rechnung neu entstehenden Formel die Grösse φ_1, φ_2 oder φ_3 wie eine neue, mit der anfänglich ebenso bezeichneten gar nicht identische Grösse ansähe.

Kehren wir jetzt zur Fortsetzung unserer Rechnung zurück. Nach Gl. (10) hat man für

$$\varphi_1 = 1,\ \varphi_2 = 1,\ \varphi_3 = 0 \text{ das } min\ w_2 = -\frac{163}{3} = -54\tfrac{1}{3}$$

$$\varphi_1 = 0,\ \varphi_2 = 0,\ \varphi_3 = 1 \text{ das } max\ w_2 = 70$$

genau so wie in §. 49. Hiernach ist

(11) $$w_2 = -\frac{163}{3} + \frac{373}{3}\psi$$

Für einen speziellen Werth von w_2 erhält man aus Gl. (7), (8), (9) das Minimum und Maximum von w_1. Um derartige Ermittelungen für verschiedene Werthe von w_2 mit Leichtigkeit anstellen zu können, ist es bequemer, die eben genannten drei Gleichungen, in deren jeder zwei Veränderliche von φ_1, φ_2, φ_3 vorkommen, erst in die Grundform (*A*) mit nur Einer solchen Veränderlichen zu bringen. Dies ist leicht, wenn man erst das Minimum und Maximum der obigen Ausdrücke für w_1 ermittelt. So hat man z. B. für den Ausdruck (8), welches auch der Werth von w_2 sein möge für

$$\varphi_1 = 1,\ \varphi_3 = 0 \text{ das } min\ w_1 = \frac{-2w_2 - 27}{7}$$

$$\varphi_1 = 0,\ \varphi_3 = 1 \text{ das } max\ w_1 = \frac{-2w_2 + 42}{7}, \text{ mithin}$$

$$w_1 = -\frac{2w_2 + 27}{7} + \frac{69}{7}\varphi'$$

Ebenso ist mit den Ausdrücken (7) und (9) zu verfahren. Hiernach kann man statt (7), (8), (9) auch schreiben

(12) $$w_1 = w_2 - 84 + 150\varphi'$$

(13) $$w_1 = -\frac{2w_2+27}{7} + \frac{69}{7}\varphi''$$

(14) $$w_1 = -\frac{3w_2+48}{12} + \frac{115}{12}\varphi'''$$

Diese drei Formeln sind es, welche, wenn sie statt der Gleichungen (7), (8), (9) zur ferneren Bestimmung der Grösse w_2 zu Grunde gelegt worden wären, hierfür nicht den einzigen Werth (10), sondern drei verschiedene Werthe geliefert haben würden, welche den dafür in §. 49 gefundenen drei Gränzbedingungen entsprechen.

Die Formeln (4), (5), (6) bedürfen einer solchen Umformung nicht, da nur Eine Veränderliche in jeder derselben vorkommt, und es daher leicht sein wird, nach vorgängiger Substitution zweier speziellen Werthe von w_2 und w_1 daraus die zugehörigen Werthe von w zu bestimmen, selbst wenn Gl. (5) nicht der Grundform (A), sondern der Grundform (B) angehört.

Für den speziellen Werth von $w_2 = 10$ hat man z. B. nach (12), (13), (14)

$w_1 = -74 + 150\varphi'$ also *min* $w_1 = -74$, *max* $w_1 = 76$,

$w_1 = -\frac{47}{7} + \frac{69}{7}\varphi''$ *min* $w_1 = -6\frac{5}{7}$, *max* $w_1 = 3\frac{1}{7}$

$w_1 = -\frac{78}{12} + \frac{115}{12}\varphi'''$ *min* $w_1 = -6\frac{1}{2}$, *max* $w_1 = 3\frac{1}{12}$

folglich in Berücksichtigung aller Bedingungen, wie in §. 49

$$min\ w_1 = -6\tfrac{1}{2},\ max\ w_1 = 3\tfrac{1}{12}$$

Für die speziellen Werthe $w_2 = 10$, $w_1 = 1$ erhält man aus (4), (5), (6)

$w = -7 + 5\varphi_1$ also *min* $w = -7$, *max* $w = -2$

$w = -2 - 5\varphi_2$ *min* $w = -7$, *max* $w = -2$

$w = -20 + 18\varphi_3$ *min* $w = -20$, *max* $w = -2$

folglich in Berücksichtigung aller Bedingungen, wie in §. 49

$$min\ w = -7,\ max\ w = -2$$

Beispiel 3. Wären im vorstehenden Beispiele, wie im Beispiele 6 des §. 49, zwischen den 3 Unbekannten w, w_1, w_2 nur die beiden Gleichungen (1), (2) gegeben; so würde eine Auflösung für w die beiden Gleichungen (4), (5) ergeben, und hieraus würde die einzige Gleichung (7) folgen, welche den Schluss der Rechnung macht.

Es ist klar, dass alsdann die Unbekannte w_2 vollkommen willkürlich bleibt, dass man aber zur Ermittelung zusammengehöriger spezieller Werthe von w, w_1, w_2, nach den erläuterten Prinzipien zu verfahren hat.

Beispiel 4. Die zwischen y und w gegebenen drei Bedingungen im Beispiele 2, §. 49 sind gleichbedeutend mit

(1) $$655 + 31440y + 1311w = 24\varphi_1$$
(2) $$5 + 240y + 10w = U\varphi_2$$
(3) $$y = U\varphi_3$$

Lös't man für w auf; so kommt

(4) $$w = \frac{-31440y - 655 + 24\varphi_1}{1311}$$
(5) $$w = \frac{-240y - 5 + U\varphi_2}{10}$$

Setzt man diese beiden Werthe von w einander gleich, lös't die entstehende Gleichung für y auf und notirt darunter nochmals die gegebene Gleichung (3); so erhält man

(6) $$y = \frac{-5 - 240\varphi_1 + 1311\,U\varphi_2}{240}$$
(7) $$y = U\varphi_3$$

Jenachdem man y durch Gl. (6) oder (7) gegeben denkt, hat man aus (6) für $\varphi_1 = 1$, $\varphi_2 = 0$ das *min* $y = -\frac{245}{240} = -1\frac{1}{48}$

für $\varphi_1 = 0$, $\varphi_2 = 1$ das *max* $y = U_1$

aus (7) für $\varphi_3 = 0$ das *min* $y = 0$

für $\varphi_3 = 1$ das *max* $y = U$

Unter Berücksichtigung aller dieser Bedingungen hat man *min* $y = 0$ *max* $y = U$ also

(8) $$y = U\psi$$

sodass $y = 0, 1, 2 \ldots \infty$ sein kann.

Beispiel 5. Nach dem Beispiele 3, §. 49 hat man zwischen x und w die drei Beziehungen

(1) $$4 + x - 7w = U\varphi_1$$
(2) $$71 - 20x + 40w = U\varphi_2$$
(3) $$x = U\varphi_3$$

Lös't man für w auf; so kommt

(4) $$w = \frac{x + 4 - U\varphi_1}{7}$$
(5) $$w = \frac{20x - 71 + U\varphi_2}{40}$$

Setzt man diese beiden Werthe einander gleich, und lös't für x auf; so hat man, wenn man auch die gegebene Gl. (3) nochmals notirt,

(6) $$x = \frac{657 - 40\,U\varphi_1 - 7\,U\varphi_2}{100}$$
(7) $$x = U\varphi_3$$

Dies gibt

aus (6) für $\varphi_1 = 1$, $\varphi_2 = 1$ das *min* $x = -U_1$

für $\varphi_1 = 0$, $\varphi_2 = 0$ das *max* $x = \frac{657}{100} = 6\frac{57}{100}$

aus (7) für $\varphi_2 = 0$ das $min\ x = 0$
für $\varphi_2 = 1$ das $max\ x = U$

also unter Berücksichtigung aller Bedingungen

$$min\ x = 0 \qquad max\ x = 6\frac{57}{100} \quad \text{also}$$

(8) $$x = \frac{657}{100}\psi$$

Für den speziellen Werth $x = 3$ hat man nach (4) und (5)

(9) $$w = \frac{7 - U\varphi_1}{7}$$

(10) $$w = \frac{-11 + U\varphi_2}{40}, \quad \text{Dies gibt}$$

aus (9) für $\varphi_1 = 1$ das $min\ w = -U_1$
für $\varphi_1 = 0$ das $max\ w = 1$
aus (10) für $\varphi_2 = 0$ das $min\ w = -\frac{11}{40}$
für $\varphi_2 = 1$ das $max\ w = +U_2$

folglich unter Berücksichtigung aller Bedingungen

$$min\ w = -\frac{11}{40}, \quad max\ w = 1$$

sodass zu dem Werthe $x = 3$ nur die beiden ganzen Werthe $w = 0, 1$ gehören können, was auch in §. 49 gefunden ist.

§. 56. *Anwendung der Gleichungen mit begränzt Veränderlichen auf die Lösung verschiedener anderer arithmetischen Aufgaben, deren Elemente zwischen gegebenen Gränzen unbestimmt gelassen sind.*

Die in Rede stehenden Ausdrücke gewähren mancherlei Vortheile bei solchen Aufgaben überhaupt, in denen nicht genau bekannte, aber gleichwol zwischen bestimmte Gränzen eingeschlossene Daten gegeben sind. Einige Beispiele werden Dies erläutern.

Aufgabe 1. Die Stärke eines Heeres ist abgeschätzt auf 80 bis 85 Bataillone à 900 bis 1000 Mann. Wie viel Mann ist dieses Heer mindestens und höchstens stark?

Hiernach sind vorhanden

$$80 + (85 - 80)\varphi = 80 + 5\varphi \text{ Bataillone,}$$

ein jedes $900 + (100 - 900)\varphi_1 = 900 + 100\varphi_1$ Mann stark.

Die Stärke x des Heeres ist also

$$x = (80 + 5\varphi)\ (900 + 100\varphi_1)$$

Demnach hat man für

$\varphi = 0,\ \varphi_1 = 0$ das $min\ x = 80 . 900 = 72000$
$\varphi = 1,\ \varphi_1 = 1$ das $max\ x = 85 . 1000 = 85000$, folglich

$$x = 72000 + 13000\psi$$

Das Heer ist also 72000 bis 85000 Mann stark.

Aufgabe 2. Man weiss, dass eine Kriegsmacht aus 80 Bataillonen à 900 bis 950 Mann besteht. Diese Macht erscheint jetzt in Korps von 6000 bis 6500 Mann im Felde. Auf wieviel derartige Korps ist mindestens und höchstens zu rechnen?

Hiernach hat man

Stärke Eines Bataillons $= 900 + 50\varphi$

Stärke von 80 Bataillonen $= 80\,(900 + 50\varphi)$

Stärke Eines Korps $= 6000 + 500\,\varphi_1$

Stärke von x Korps $= x\,(6000 + 500\,\varphi_1)$

$$x\,(6000 + 500\,\varphi_1) = 80\,(900 + 50\,\varphi)$$

$$x = \frac{80\,(900 + 50\,\varphi)}{6000 + 500\,\varphi_1} = \frac{144 + 8\,\varphi}{12 + \varphi_1}$$

für $\varphi = 0,\ \varphi_1 = 1$ das *min* $x = \frac{144}{13} = 11\frac{1}{13}$

für $\varphi = 1,\ \varphi_1 = 0$ das *max* $x = \frac{38}{3} = 12\frac{2}{3}$

Das Heer besteht also aus 11 bis 13 Korps.

Aufgabe 3. Bei einem Geschäfte sind 30000 bis 40000 Thlr. zu gewinnen. Von 4 Unternehmern *A, B, C, D* glaubt

A) 10000 bis 11000 Thlr.
B) 3000 bis 4000 Thlr.
C) höchstens 1500 Thlr.
D) 9000 Thlr.

zu den erforderlichen Betriebskosten beisteuern zu können. Welche Rechnung wird sich jeder Unternehmer mindestens und höchstens auf den Gewinn machen können?

Man hat folgende Einlagen

		:500
von	$A = 10000 + 1000\,\varphi_1$	$20 + 2\,\varphi_1$
»	$B = 3000 + 1000\,\varphi_2$	$6 + 2\,\varphi_2$
»	$C = 1500\,\varphi_3$	$3\,\varphi_3$
»	$D = 9000$	18
	Summa =	$44 + 2\,\varphi_1 + 2\,\varphi_2 + 3\,\varphi_3$

Hiernach wird der Antheil an dem Gewinne von $30000 + 10000\varphi$ Thalern sein

$$\text{für } A = \left(\frac{20 + 2\,\varphi_1}{44 + 2\,\varphi_1 + 2\,\varphi_2 + 3\,\varphi_3}\right)(30000 + 10000\,\varphi)$$

$$\text{» } B = \left(\frac{6 + 2\,\varphi_2}{44 + 2\,\varphi_1 + 2\,\varphi_2 + 3\,\varphi_3}\right)(30000 + 10000\,\varphi)$$

$$\text{» } C = \left(\frac{3\,\varphi_3}{44 + 2\,\varphi_1 + 2\,\varphi_2 + 3\,\varphi_3}\right)(30000 + 10000\,\varphi)$$

$$\text{» } D = \left(\frac{18}{44 + 2\,\varphi_1 + 2\,\varphi_2 + 3\,\varphi_3}\right)(30000 + 10000\,\varphi)$$

Dies gibt zuvörderst, wenn man noch in jedem Gewinne diejenige der Grössen φ_1, φ_2, φ_3, welche zugleich im Zähler und

Nenner erscheint, unbestimmt lässt, und dieselbe dann durch Anwendung der Formel $\frac{M+z}{N+z}=1-\frac{N-M}{N+z}$ bloss in den Nenner schafft, für

$\varphi=0,\ \varphi_2=1,\ \varphi_3=1$ das *min* $A=\left(\frac{20+2\varphi_1}{49+2\varphi_1}\right)30000=\left(1-\frac{29}{49+2\varphi_1}\right)30000$

$\varphi=1,\ \varphi_2=0,\ \varphi_3=0$ das *max* $A=\left(\frac{20+2\varphi_1}{44+2\varphi_1}\right)40000=\left(1-\frac{12}{22+\varphi_1}\right)40000$

$\varphi=0,\ \varphi_1=1,\ \varphi_3=1$ das *min* $B=\left(\frac{6+2\varphi_2}{49+2\varphi_2}\right)30000=\left(1-\frac{43}{49+2\varphi_2}\right)30000$

$\varphi=1,\ \varphi_1=0,\ \varphi_3=0$ das *max* $B=\left(\frac{6+2\varphi_2}{44+2\varphi_2}\right)40000=\left(1-\frac{19}{22+\varphi_2}\right)40000$

$\varphi=0,\ \varphi_1=1,\ \varphi_2=1$ das *min* $C=\left(\frac{3\varphi_3}{48+3\varphi_3}\right)30000=\left(1-\frac{16}{16+\varphi_3}\right)30000$

$\varphi=1,\ \varphi_1=0,\ \varphi_2=0$ das *max* $C=\left(\frac{3\varphi_3}{44+3\varphi_3}\right)40000=\left(1-\frac{44}{44+3\varphi_3}\right)40000$

$\varphi=0,\ \varphi_1=1,\ \varphi_2=1,\ \varphi_3=1$ das *min* $D=\frac{6}{17}.\ 30000$

$\varphi=1,\ \varphi_1=0,\ \varphi_2=0,\ \varphi_3=0$ das *max* $D=\frac{9}{22}.\ 40000$

Hieraus folgt nun ferner für

$\varphi_1=0$ das *min* $A=\frac{20}{49}.30000=12244\frac{44}{49}$

$\varphi_1=1$ das *max* $A=\frac{22}{46}.40000=19130\frac{10}{23}$

$\varphi_2=0$ das *min* $B=\frac{6}{49}.30000=\ 3673\frac{23}{49}$

$\varphi_2=1$ das *max* $B=\frac{8}{46}.40000=\ 6956\frac{12}{23}$

$\varphi_3=0$ das *min* $C=\ 0\ .30000=\ 0$

$\varphi_3=1$ das *max* $C=\frac{3}{47}.40000=\ 2553\frac{9}{47}$

das *min* $D=\frac{6}{17}.30000=10588\frac{4}{17}$

das *max* $D=\frac{9}{22}.40000=16363\frac{7}{11}$

Bei Weglassung der Brüche wird also

A	mindestens	12244	und höchstens	19130	Thlr.	gewinnen
B	»	3673	» »	6956	»	»
C			»	2553	»	»
D	»	10588	» »	16363	»	»

Aufgabe 4. Was war zu einer Zeit der Preis des 12löthigen Silbers pro Mark, als das Pfund Silber 36 bis 40 Thlr. und das Pfund Kupfer 10 bis 12 Ggr. kostete?

Man hatte zu der fraglichen Zeit

Preis von 1 Loth Silber $= \frac{1}{32}(36 + 4\varphi_1)$ Thaler

» » » » Kupfer $= \frac{1}{32}\left(\frac{5}{12} + \frac{1}{12}\varphi_2\right)$ »

Es war also der Preis x von 12 Loth Silber und 4 Loth Kupfer oder von 1 Mark 12löthigem Silber

$$x = \frac{12}{32}(36 + 4\varphi_1) + \frac{4}{32}\left(\frac{5}{12} + \frac{1}{12}\varphi_2\right)$$

$$= \frac{1301}{96} + \frac{3\varphi_1}{2} + \frac{\varphi_2}{96}$$

Demnach ist für

$\varphi_1 = 0,\ \varphi_2 = 0$ das *min* $x = \frac{1301}{96}$ Thlr. $=$ 13 Thlr. 13 Ggr. 3 Pf.

$\varphi_1 = 1,\ \varphi_2 = 1$ das *max* $x = \frac{1350}{96}$ Thlr. $=$ 14 Thlr. 1 Ggr.

Der gesuchte Preis war also 13 Thlr. 13 Ggr. 3 Pf. bis 14 Thlr. 1 Ggr.

Aufgabe 5. Ein Grundstück von 20 bis 22 Morgen sollte für 2500 Thlr. verkauft werden. Jetzt ist dasselbe um 5 Morgen vergrössert; was wird nun der Preis für das vergrösserte Grundstück sein?

Man hat

frühere Grösse des Grundstücks $= 20 + 2\varphi$ Morgen,
jetzige » » » $= 25 + 2\varphi$ »

Der Preis x für das vergrösserte Grundstück ist also

$$x = \left(\frac{25 + 2\varphi}{20 + 2\varphi}\right)2500 = \left(1 + \frac{5}{20 + 2\varphi}\right)2500,$$ also für

$\varphi = 1$ das *min* $x = \frac{27}{22}.2500 = 3068\frac{2}{11}$

$\varphi = 0$ das *max* $x = \frac{25}{20}.2500 = 3125$

Der Preis für das vergrösserte Grundstück beträgt also $3068\frac{2}{11}$ bis 3125 Thlr.

Aufgabe 6. Es werden miteinander vermischt

200 Kubikfuss einer Flüssigkeit, deren spezifisches Gewicht $= 0,5$ ist
100 » » » » » » $= 1,5$ »

Bei der Inhaltsmessung können Fehler bis zu dem Betrage von 3 Prozent, und bei der Ermittelung des spezifischen Gewichtes Fehler bis zu 2 Prozent untergelaufen sein, sodass der wahre Inhalt und das wahre spezifische Gewicht der Flüssigkeiten möglicherweise um die genannten Prozente kleiner oder grösser sein können, als die gegebenen Zahlen. Es wird nach dem spezifischen Gewichte der Mischung gefragt.

Hiernach besitzt die erste Flüssigkeit ein Volum mindestens von 194 und höchstens von 206, also von $194 + 12\varphi_1$ Kubikfuss, und ein spezifisches Gewicht mindestens von 0,49 und höchstens von 0,51, also von $0,49 + 0,02\varphi_1$.

Die zweite Flüssigkeit besitzt ein Volum mindestens von 97 und höchstens von 103, also von $97 + 6\varphi_2$ Kubikfuss, und ein spezifisches Gewicht mindestens von 1,47 und höchstens von 1,53, also von $1,47 + 0,06\psi_2$.

Hiernach ist das absolute Gewicht der ersten Flüssigkeit gleich dem Gewichte von $(194 + 12\varphi_1)(0,49 + 0,02\psi_1)$ Kubikfuss Wasser, und das der zweiten Flüssigkeit gleich dem Gewichte von $(97 + 6\varphi_2)(1,47 + 0,06\psi_2)$ Kubikfuss Wasser.

Das spezifische Gewicht x der Mischung ist mithin

$$x = \frac{(194 + 12\varphi_1)(0,49 + 0,02\psi_1) + (97 + 6\varphi_2)(1,47 + 0,06\psi_2)}{(194 + 12\varphi_1) + (97 + \varphi_2)}.$$

Zuvörderst erhellet, dass man für das *min* x stets $\psi_1 = 0$, $\psi_2 = 0$ und für das *max* x stets $\psi_1 = 1$, $\psi_2 = 1$ haben müsse, welches auch die Werthe der übrigen Veränderlichen seien. Dies gibt für

$$\psi_1 = 0,\ \psi_2 = 0 \text{ das } \min x = \frac{23765 + 588\varphi_1 + 882\varphi_2}{300(97 + 4\varphi_1 + 2\varphi_2)}$$

$$\psi_1 = 1,\ \psi_2 = 1 \text{ das } \max x = \frac{8245 + 204\varphi_1 + 306\varphi_2}{100(97 + 4\varphi_1 + 2\varphi_2)}$$

Das Minimum lässt sich, jenachdem man eine theilweise Division des Nenners in den Zähler mit $4\varphi_1$ oder mit $2\varphi_2$ ausführt, resp. in die Form

$$\min x = \frac{1}{300}\left(147 + \frac{9506 + 588\varphi_2}{97 + 4\varphi_1 + 2\varphi_2}\right)$$

oder in die Form

$$\min x = \frac{1}{300}\left(441 - \frac{19012 + 1176\varphi_1}{97 + 4\varphi_1 + 2\varphi_2}\right)$$

bringen. Aus der ersteren erkennt man, dass das Minimum die Bedingung $\varphi_1 = 1$ erfordert, welches auch der Werth von φ_2 sei, und aus der letzteren geht hervor, dass das Minimum die Bedingung $\varphi_2 = 0$ erfordert, welches auch der Werth von φ_1 sei. Man hat also für das Minimum $\varphi_1 = 1$, $\varphi_2 = 0$ zu nehmen.

Was das Maximum betrifft; so lässt sich dasselbe, jenachdem man eine theilweise Division des Nenners in den Zähler mit $4\varphi_1$ oder mit $2\varphi_2$ ausführt, resp. in die Form

$$\max x = \frac{1}{100}\left(51 + \frac{3298 + 204\varphi_2}{97 + 4\varphi_1 + 2\varphi_2}\right)$$

oder in die Form

$$\max x = \frac{1}{100}\left(153 - \frac{6596 + 408\varphi_1}{97 + 4\varphi_1 + 2\varphi_2}\right)$$

bringen. Aus der ersteren erkennt man, dass $\varphi_1 = 0$ sein muss, welches auch der Werth von φ_2 sei, und aus der letzteren folgt $\varphi_2 = 1$, welches auch der Werth von φ_1 sei. Das Maximum verlangt also die beiden Bedingungen $\varphi_1 = 0$, $\varphi_2 = 1$.

Hiernach hat man nun für

$$\varphi_1 = 1,\ \varphi_2 = 0 \text{ das } min\ x = \frac{24353}{30300} = 0{,}803729\ldots$$

$$\varphi_1 = 0,\ \varphi_2 = 1 \text{ das } max\ x = \frac{8551}{9900} = 0{,}863737\ldots$$

Das spezifische Gewicht der Mischung liegt also zwischen 0,8037 . . . und 0,8637 . . .

Hätte man auf die Ungenauigkeiten der Messungen gar keine Rücksicht genommen; so würde Dies für die Mischung das spezifische Gewicht 0,8333 . . . ergeben haben.

Vierter Abschnitt.

Unendliche periodische Kettenbrüche.

§. 57. *Allgemeine Bemerkungen über unendliche Kettenbrüche.*

I. Die im ersten Abschnitte nachgewiesenen Beziehungen zwischen den Näherungswerthen eines endlichen Kettenbruchs gelten offenbar auch von den Näherungswerthen eines unendlichen Kettenbruchs, insofern die fraglichen Gesetze unabhängig sind von den Quotienten, welche das Ende des Kettenbruchs bilden, oder von dem Gesammtwerthe dieses Kettenbruchs. Der Anfang eines unendlichen Kettenbruchs kann ja immer wie der Anfang eines endlichen Kettenbruchs betrachtet werden.

Man weiss, dass die sukzessiven Näherungswerthe eines nach dem Additionsprinzipe gebildeten Kettenbruches mit lauter positiven oder mit lauter negativen Quotienten sich fortwährend einem bestimmten Werthe nähern. Wenn nun die Quotienten eines unendlichen Kettenbruchs von einer gewissen Stelle an ins Unendliche fort sämmtlich positiv oder sämmtlich negativ sind, ohne den Werth null zu enthalten; so müssen von dieser Stelle an die weiter folgenden Näherungswerthe sich fortwährend einem bestimmten Werthe bis zu jeder beliebigen Kleinheit der Fehlergränze nähern. Diese Grösse ist natürlich der Gesammtwerth des unendlichen Kettenbruchs. Ein Kettenbruch von der bezeichneten Art kann also ein konvergenter genannt werden.

Die Richtigkeit dieser Behauptung erhellet, wenn man beachtet, dass man bei der Bezeichnung des §. 3 ebenso wie in §. 6, indem K den Werth des unendlichen Kettenbruchs, n den Zeiger eines Näherungswerthes und r den Zeiger eines späteren Näherungswerthes bezeichnet,

$$K_r - K_n = \frac{(-1)^n}{N_n\,(N_{n+1} + N_n\, x_{n+1})}$$

hat. Hierin ist $x_{n+1} = [0,\, a_{n+2},\, a_{n+3},\, a_{n+4},\, \ldots\, a_r]$. Lässt man hierin r wachsen; so ändert sich auf der rechten Seite der vorstehenden Gleichung nur die Grösse x_{n+1}. Sind aber von einer gewissen Stelle an alle Quotienten bis ins Unendliche fort nur positiv oder nur negativ, und liegt a_{n+2} unterhalb jener Stelle; so nähert sich die Grösse x_{n+1}, welche selbst einen den Bedingungen des ersten Abschnitts entsprechenden Kettenbruch darstellt, fortwährend bis zu jedem Grade der Genauigkeit einem bestimmten Werthe, je grösser man r nimmt.

Nach der Zusammensetzung der vorstehenden Formel ist klar, dass unter diesen Umständen auch der Werth der Differenz $K_r - K_n$ sich einem bestimmten Werthe ins Unendliche nähert, wenn r fortwährend wächst. Für $r = \infty$ ist aber $K_\infty = K$ der Gesammtwerth des unendlichen Kettenbruchs. Es stellt also K_r diesen Gesammtwerth immer genauer dar, je tiefer r unter der bezeichneten Stelle genommen wird.

II. Was nun den genauen Werth eines unendlichen Kettenbruchs von der bezeichneten Art betrifft; so leuchtet zuvörderst ein, dass derselbe irrational sein muss. Dies kann man sowol daraus folgern, dass Zähler und Nenner der Näherungsbrüche ins Unendliche wachsen und stets relativ prim bleiben, wie auch aus folgender Betrachtung. Hätte K den Werth eines rationalen Bruches; so müsste es möglich sein, denselben in der Form des gegebenen unendlichen Kettenbruchs zu entwickeln. Beginnt man nun, jenen rationalen Bruch in einen Kettenbruch zu verwandeln; so kann man jederzeit zu den ersten Quotienten von den Zeigern 0, 1, 2 ... n die Quotienten $a_0, a_1, a_2, \ldots a_n$ des unendlichen Kettenbruchs nehmen, gleichviel ob dieselben grösste Sub- oder kleinste Super- oder willkürliche Quotienten sind. Damit nun aber bei der ferneren Entwickelung als $a_{n+2}, a_{n+3}, \ldots$ in inf. entweder lauter positive Zahlen > 0 oder lauter negative Zahlen < 0 erscheinen können, ist es nach §. 18 unerlässlich, dass man vom Index $n+1$ an die Entwickelung entweder mit grössten Sub- oder mit kleinsten Superquotienten ohne eine einzige Abweichung von dieser Regel fortsetze. Bei diesem Verfahren muss aber die Entwickelung endlich abbrechen; es ist also unmöglich, dass sich ein unendlicher Kettenbruch erzeuge.

Im Allgemeinen, wenn die Quotienten eines unendlichen Kettenbruchs kein bekanntes oder doch ein komplizirtes Gesetz befolgen, lässt sich der genaue Werth dieses Bruches in geschlossener Form nicht darstellen. Man kann sich demselben durch die sukzessiven Näherungsbrüche nur bis zu jedem Grade der Genauigkeit nähern. Hierbei ist zu beachten, dass wenn alle Quotienten des unendlichen Kettenbruchs positiv und > 0 oder negativ und < 0 sind, wobei indessen für den obersten a_0 der Werth null zulässig ist, die aufeinander folgenden Näherungswerthe abwechselnd grösser und kleiner sind, als der genaue Werth des unendlichen Kettenbruchs, und dass die Fehlergränze ein Bruch mit der Einheit zum Zähler und dem Quadrate des Nenners des betreffenden Näherungsbruchs zum Nenner ist (§. 6)

Von besonderer Wichtigkeit ist jedoch der Fall, wo die Quotienten eines unendlichen Kettenbruchs von einer gewissen Stelle an regelmässig wiederkehren oder eine Periode bilden. Ein solcher Kettenbruch lässt sich immer, die Quotienten mögen positiv oder negativ oder Beides zugleich sein, genau reduziren, wie im nachstehenden Paragraphen gelehrt werden soll.

§. 58. Reduktion eines periodischen Kettenbruchs.

I. Angenommen, in dem nach dem Additionsprinzipe gebildeten unendlichen Kettenbruche $K = [a_0, a_1, a_2 \ldots a_n, a_{n+1}, \ldots a_{n+r}, a_{n+r+1}, \ldots]$ wiederholen sich die r Quotienten $a_{n+1} \ldots a_{n+r}$ in derselben Reihenfolge unausgesetzt, sodass $a_{n+r+1}, a_{n+r+2} \ldots$ resp. $= a_{n+1}, a_{n+2} \ldots$ ist.

Unter diesen Umständen stellen irgend zwei mit den Anfangsgliedern zweier beliebigen Perioden beginnende untere Theile des gegebenen Kettenbruchs zwei einander vollkommen identische unendliche Kettenbrüche dar. Demnach hat der Gesammtbetrag eines jeden solchen Theiles Ein und denselben, wenn auch irrationalen Werth, welchen wir mit x bezeichnen wollen. Es ist also $x = [a_{n+1}, a_{n+2} \ldots] = [a_{n+r+1}, a_{n+r+2} \ldots] = [a_{n+2r+1}, a_{n+2r+2} \ldots] =$ etc.

Hieraus ist klar, dass wenn man die Irrationalzahl x als den letzten Quotienten eines endlichen Kettenbruchs ansieht, man den Werth K des gegebenen Kettenbruchs sowol durch

(1) $\quad K = [a_0, a_1, a_2 \ldots a_n, x]$ als auch durch

(2) $\quad K = [a_0, a_1, a_2 \ldots a_{n+r}, x]$

darstellen kann.

Zufolge §. 3 hat man nach dem ersten Ausdrucke für K

(3) $\quad K = \dfrac{x M_n + M_{n-1}}{x N_n + N_{n-1}}$ und nach dem zweiten Ausdrucke

(4) $\quad K = \dfrac{x M_{n+r} + M_{n+r-1}}{x N_{n+r} + N_{n+r-1}}$

Eliminirt man zwischen diesen beiden Gleichungen die Grösse x; so ergibt sich folgende Gleichung

$$(5)\quad \begin{cases} (N_{n-1}\,N_{n+r} - N_n\,N_{n+r-1})K^2 \\ -(M_{n-1}\,N_{n+r} + M_{n+r}\,N_{n-1} - M_n\,N_{n+r-1} - M_{n+r-1}\,N_n)K \\ +(M_{n-1}\,M_{n+r} - M_n\,M_{n+r-1}) = 0 \end{cases}$$

Dies ist eine quadratische Gleichung von der Form

$$fK^2 - gK + h = 0$$

aus welcher sich der Werth von K in der Form

$$(6)\qquad K = \frac{\pm\sqrt{g^2 - 4fh} + g}{2f} = \frac{\pm\sqrt{D} + P}{Q}$$

ergibt. Man erkennt also, dass der Werth eines unendlichen periodischen Kettenbruchs der bezeichneten Art gleich der Wurzel einer unreinen quadratischen Gleichung ist. Aus der Natur der Sache folgt, dass $D = g^2 - 4fh$ weder eine vollkommene Quadratzahl (mithin auch nicht $= 0$), noch negativ sein kann, weil K im ersteren Falle einen rationalen und im letzteren einen imaginären Werth haben würde, was Beides unter den gegebenen Umständen unmöglich ist.

II. Da man annehmen kann, dass jede spätere Periode von K die erste sei; so kann man in der Gl. (5) statt n jeden Werth von der Form $n + pr$ setzen, worin p eine positive ganze Zahl bezeichnet. Da man ferner annehmen kann, dass jede beliebige Menge jener $r$gliedrigen Perioden Eine Periode bilden; so kann man in der Gl. (5) für r auch jeden Werth von der Form qr setzen, worin q eine positive ganze Zahl bezeichnet.

Die Rechnung wird jedoch immer am kürzesten sein, wenn man $p = 0$ und $q = 1$ nimmt.

Da das Bildungsgesetz der Zähler und Nenner der Näherungsbrüche aus §. 3, auf welchem die Gleichungen (3), (4), (5) beruhen, schon mit dem Zeiger 0 beginnt, sodass man $M_0 = a_0\,M_{-1} + M_{-2}$ und $N_0 = a_0\,N_{-1} + N_{-2}$ hat; so ist die Gl. (5) in allen Fällen anwendbar, wo $n - 1$ nicht kleiner als -2, oder n nicht kleiner als -1, also der Zeiger $n + 1$ des Anfangsgliedes der ersten Periode nicht kleiner als 0 ist. Der entgegengesetzte Fall kann aber niemals eintreten; die Gl. (5) ist also in allen Fällen brauchbar.

Wäre z. B. $K = [\overset{0}{2}, \overset{1}{7}, \underbrace{\overset{2}{4}, \overset{3}{8}}, \underbrace{\overset{4}{4}, \overset{5}{8}} \ldots]$ gegeben, wo die zweigliedrige Periode 4, 8 mit dem Zeiger 2 beginnt, also $n = 1$, $r = 2$ ist; so hat man nach Gl. (5)

$$(N_0\,N_3 - N_1\,N_2)K^2 - (M_0\,N_3 + M_3\,N_0 - M_1\,N_2 - M_2\,N_1)K$$
$$+ (M_0\,M_3 - M_1\,M_2) = 0$$

Um die hierin vorkommenden Zähler und Nenner der Näherungsbrüche zu bestimmen, hat man

n	a_n	M_n	N_n
−2		0	1
−1		1	0
0	2	2	1
1	7	15	7
2	4	62	29
3	8	511	239

$$(1.239 - 7.29)K^2 - (2.239 + 511.1 - 15.29 - 62.7)K$$
$$+ (2.511 - 15.62) = 0$$
$$36K^2 - 120K + 92 = 0 \text{ also}$$
$$K = \frac{\pm\sqrt{2} + 5}{3}$$

III. Es kommt jetzt noch darauf an, das Zeichen der zweideutigen Quadratwurzel $\pm\sqrt{D}$ zu bestimmen.

Zu diesem Ende ist nur zu entscheiden, ob nach der Bezeichnung in Gl. (6) $K >$ oder $< \frac{P}{Q}$ d. i. $>$ oder $< \frac{g}{2f}$ ist. Dies kann jederzeit leicht durch folgende Betrachtung ermittelt werden.

Die Differenz zwischen dem genauen Werthe von K nach Gl. (3) und dem Näherungsbruche $K_n = \frac{M_n}{N_n}$ ist, indem sich der Zeiger n nicht nothwendig auf den der ersten Periode vorhergehenden Quotienten, sondern auf einen beliebigen zu beziehen braucht, sodass dann immer $x = [a_{n+1}, a_{n+2} \ldots]$ ist,

$$(7) \qquad K - K_n = \frac{xM_n + M_{n-1}}{xN_n + N_{n-1}} - \frac{M_n}{N_n} = \frac{(-1)^n}{N_n(xN_n + N_{n-1})}$$

Setzen wir nun voraus, der Zeiger n liege in irgend Einer der Perioden, und die periodischen Quotienten $a_{n+1}, a_{n+2}, \ldots$ seien entweder sämmtlich positiv oder sämmtlich negativ. Sind sie positiv; so ist $x > 1$: sind sie negativ; so ist $x < -1$, sodass der numerische Werth von x jederzeit > 1 ist. Es leuchtet ein, dass von irgend einem Zeiger an die Werthe der Nenner N der Näherungsbrüche ihrem numerischen Werthe nach in beiden Fällen fortwährend wachsen werden. Diese Stelle wird leicht zu erkennen sein, wenn man die sukzessiven Näherungswerthe von K oder auch nur die sukzessiven Werthe der Nenner N herstellt. Es sei N_{n-1} ein solcher in den wachsenden Werthen von N liegender Nenner.

IV. Sind nun die Quotienten $a_{n+1}, a_{n+2} \ldots$ sämmtlich positiv, also $x > 1$; so haben alle Grössen $N_{n-1}, N_n, N_{n+1} \ldots$ einerlei Zeichen. Es ist also für n und jeden höheren Zeiger $N_n(xN_n + N_{n-1})$ positiv und auch $> N_n^2$. Sind dagegen die Quotienten $a_{n+1}, a_{n+2} \ldots$ sämmtlich negativ, also $x < -1$; so haben je zwei benachbarte Grössen in der Reihe $N_{n-1}, N_n, N_{n+1} \ldots$ entgegengesetzte Zeichen. Es ist also für n und jeden höheren Zeiger $N_n(xN_n + N_{n-1})$ negativ und dem absoluten

Werthe nach $> N_n^2$. Folglich ist in beiden Fällen der absolute Werth von $\frac{1}{N_n(xN_n + N_{n-1})} < \frac{1}{N_n^2}$.

Ausserdem wechselt die Differenz $K - K_n$, wenn n um 1 wächst, immer das Zeichen, d. h. K_n ist abwechselnd grösser und kleiner, als der wahre Werth K des unendlichen Kettenbruchs, jedoch niemals um den vollen Betrag des immer kleiner werdenden Bruches $\frac{1}{N_n^2}$.

Hieraus folgt, dass endlich einmal unterhalb der vorhin bezeichneten Stelle zwei unmittelbar aufeinander folgende Näherungsbrüche, etwa K_m und K_{m+1}, und demnach auch alle späteren $K_{m+2}, K_{m+3} \ldots$ grösser oder kleiner werden müssen, als irgend ein Bruch $\frac{P}{Q}$, dessen Werth von K verschieden ist. Sucht man also die nächsten zwei Näherungsbrüche K_m und K_{m+1} unterhalb der genannten Stelle auf, welche beide entweder grösser oder beide kleiner sind, als $\frac{P}{Q}$; so ergibt sich daraus, dass K resp. grösser oder kleiner sei, als $\frac{P}{Q}$.

Im obigen Beispiele, wo alle Quotienten positiv sind, hat man $\frac{P}{Q} = \frac{g}{2f} = \frac{120}{2.36} = \frac{5}{3}$, und da man erkennt, dass alle Nenner schon von N_0 an fortwährend wachsen, und dass sowol $K_0 = \frac{2}{1}$, als auch $K_1 = \frac{15}{7}$ grösser als $\frac{P}{Q} = \frac{5}{3}$ ist; so folgt, dass $K > \frac{5}{3}$, also $= \frac{+\sqrt{2}+5}{3}$ und nicht $= \frac{-\sqrt{2}+5}{3}$ sei.

Wäre der Kettenbruch $K = [\underbrace{1, 2, 3,}\underbrace{1, 2, 3}\ldots]$ gegeben, worin die dreigliedrige Periode 1, 2, 3 schon mit dem Zeiger 0 beginnt; so hat man $n = -1$, $r = 3$, also nach Gl. (5)

$$(N_{-2}N_2 - N_{-1}N_1)K^2 - (M_{-2}N_2 + M_2N_{-2} - M_{-1}N_1 - M_1N_{-1})K$$
$$+ (M_{-2}M_2 - M_{-1}M_1) = 0$$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	2	3	2
2	3	10	7

$$(1.7 - 0.2)K^2 - (0.7 + 10.1 - 1.2 - 3.0)K + (0.10 - 1.3) = 0$$

$$7K^2 - 8K - 3 = 0$$

$$K = \frac{\pm\sqrt{37}+4}{7}$$

Da hier $K_0 = \frac{1}{1} > \frac{4}{7}$ und auch $K_1 = \frac{3}{2} > \frac{4}{7}$ ist; so muss $K > \frac{4}{7}$, also $K = \frac{+\sqrt{37}+4}{7}$ sein.

V. **Wären die periodischen Quotienten des gegebenen Kettenbruchs nicht sämmtlich positiv oder sämmtlich negativ; so kann die in der Gl. (7) vorkommende Grösse x zwischen zwei benachbarten Näherungsbrüchen selbst das Zeichen wechseln.** In diesem Falle hat man zur Entscheidung, ob $K >$ oder $< \frac{P}{Q}$ sei, in der vorhin beschriebenen Weise nicht die unmittelbar aufeinander folgenden, sondern die in Abständen von der Länge Einer Periode aufeinander folgenden Näherungsbrüche, für welche x immer denselben Werth haben muss, also zwei Brüche wie K_n und K_{n+r} zu prüfen.

VI. Wenn die Periode schon mit dem Zeiger 0 beginnt; so vereinfacht sich die obige Gl. (5). Wir haben alsdann $n = -1$ und wenn man den letzten Zeiger in der Periode mit m bezeichnet, also $n + r = m$, folglich $r = m - n = m + 1$ setzt, da $M_{-2} = 0$, $N_{-2} = 1$, $M_{-1} = 1$, $N_{-1} = 0$ ist,

$$(8) \qquad N_m K^2 - (M_m - N_{m-1}) K - M_{m-1} = 0 \text{ also}$$

$$(9) \qquad K = \pm \sqrt{\left(\frac{M_m - N_{m-1}}{2 N_m}\right)^2 + \frac{M_{m-1}}{N_m}} + \frac{M_m - N_{m-1}}{2 N_m}$$

Wenn die Periode mit dem Zeiger 1 beginnt, also $n = 0$ ist, wird die Gl. (5), indem der letzte Zeiger in der Periode jetzt $n + r = r$ ist, unter Beachtung der Werthe $M_0 = a_0$, $N_0 = 1$,

$$(10) \qquad -N_{r-1} K^2 - (N_r - a_0 N_{r-1} - M_{r-1}) K + (M_r - a_0 M_{r-1}) = 0 \text{ also}$$

$$(11) \qquad K = \pm \sqrt{\left(\frac{M_{r-1} - N_r + a_0 N_{r-1}}{2 N_{r-1}}\right)^2 + \frac{M_r - a_0 M_{r-1}}{N_{r-1}}} + \frac{M_{r-1} - N_r + a_0 N_{r-1}}{2 N_{r-1}}$$

So hat man z. B. für $K = [2, \underbrace{1, 1, 1, 4}, \underbrace{1, 1, 1, 4} \ldots]$, worin $n = 0$, $r = 4$ ist,

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	2	2	1
1	1	3	1
2	1	5	2
3	1	8	3
4	4	37	14

$M_{r-1} = M_3 = 8$, $N_{r-1} = N_3 = 3$
$M_r = M_4 = 37$, $N_r = N_4 = 14$

$$K = \sqrt{\left(\frac{8 - 14 + 2.3}{2.3}\right)^2 + \frac{37 - 2.8}{3}} + \frac{8 - 14 + 2.3}{2.3} = \sqrt{7}$$

Es ist übrigens nicht unbedingt nothwendig, dass die in Gl. (9) in Bruchform geschriebenen Grössen sich stets auf ganze

Zahlen reduziren. Wäre z. B. $K = [2, \underbrace{1, 3, 1, 4,} \underbrace{1, 3, 1, 4} \ldots]$ gegeben; so hätte man

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	2	2	1
1	1	3	1
2	3	11	4
3	1	14	5
4	4	67	24

$$M_{r-1} = M_3 = 14,\ N_{r-1} = N_3 = 5$$
$$M_r = M_4 = 67,\ N_r = N_4 = 24$$

$$K = \sqrt{\left(\frac{14-24+2.5}{2.10}\right)^2 + \frac{67-2.14}{5}} + \frac{14-24+2.5}{2.10}$$
$$= \sqrt{\frac{39}{5}}$$

Entwickelung irrationaler reeller Quadratwurzeln in Kettenbrüche.

§. 59. *Entwickelung der Wurzel einer quadratischen Gleichung in einen Kettenbruch mit grössten Subquotienten nach dem Additionsprinzipe.*

I. Im vorstehenden Paragraphen haben wir gefunden, dass die Reduktion eines periodischen Kettenbruchs auf den Werth $K = \frac{\sqrt{D}+P}{Q}$ führt, welcher die Wurzel einer quadratischen Gleichung darstellt. Wir wollen jetzt umgekehrt einen Ausdruck der vorstehenden Form in einen Kettenbruch verwandeln, welcher voraussichtlich periodisch sein wird. Wenn etwas Anderes nicht ausdrücklich befürwortet wird, soll die Entwickelung immer nach dem Additionsprinzipe mit grössten Subquotienten geschehen. Wir schreiben nun

$$(1) \qquad K = \frac{\sqrt{D}+P_0}{Q_0}$$

und nennen die Grösse D unter dem Wurzelzeichen, welche späterhin noch eine wichtige Rolle spielen wird, die **Determinante** des Ausdrucks K. Dieselbe wird als eine **ganze positive** Zahl, welche **kein vollkommenes** Quadrat ist, vorausgesetzt, sodass also $\sqrt{D}$ eine **irrationale reelle** Grösse ist. P_0 und Q_0 sind zwei **ganze**, aber beliebig positive oder negative Zahlen; P_0 kann auch $= 0$ sein. Es ist klar, dass gebrochene Werthe für D, P_0, Q_0 nicht betrachtet zu werden brauchen, da die etwaigen Nenner durch Multiplikation des ganzen Zählers und Nenners von K leicht beseitigt werden können.

II. Die Wurzelgrösse $\sqrt{D}$ wird nicht als zweideutig, sondern als entschieden positiv betrachtet, was der Allgemeinheit der Formel keinen Abbruch thut, da, wenn $\sqrt{D}$ negativ wäre, eine Multiplikation des Zählers und Nenners von K mit -1 jene Grösse positiv macht.

III. Endlich wird die Bedingung ausgesprochen, dass $D-P_0^2$ durch Q_0 theilbar, also $\frac{D-P_0^2}{Q_0}$ eine ganze Zahl sei, welche wir mit

(2) $$Q_{-1}=\frac{D-P_0^2}{Q_0}$$

bezeichnen. Auch hierdurch wird die Allgemeinheit der Formel nicht beeinträchtigt, indem man, wenn Q_0 nicht in $D-P_0^2$ enthalten, vielmehr m das grösste gemeinschaftliche Maass von Q_0 und $D-P_0^2$, also $Q_0=\alpha m$, $D-P_0^2=\beta m$ wäre, man durch Multiplikation des Zählers und Nenners von K mit α den Ausdruck

$$K=\frac{\sqrt{\alpha^2 D}+\alpha P_0}{\alpha Q_0}=\frac{\sqrt{D'}+P_0'}{Q_0'}$$

erhält, worin nun $Q_{-1}=\frac{D'-P_0'^2}{Q_0'}=\frac{\alpha^2 D-\alpha^2 P_0^2}{\alpha Q_0}=\frac{\alpha(D-P_0^2)}{Q_0}$ $=\frac{\alpha\beta m}{\alpha m}=\beta$ eine ganze Zahl ist.

Wollte man nicht gerade die kleinstmöglichen Zahlen haben, was übrigens für die Rechnung das Bequemste ist; so könnte man, um $D-P_0^2$ durch Q_0 theilbar zu machen, wenn Dies nicht schon von vorn herein stattfände, Zähler und Nenner von K sofort mit Q_0 multipliziren, wodurch man

$$K=\frac{\sqrt{Q_0^2 D}+Q_0 P_0}{Q_0^2}=\frac{\sqrt{D'}+P_0'}{Q_0'}$$

$$Q_{-1}=\frac{D'-P_0'^2}{Q_0'}=D-P_0^2$$

erhielte.

Der Fall $Q_0=0$, wodurch $Q_{-1}=\infty$ werden würde, ist ausgeschlossen.

IV. Es wird noch bemerkt, dass der obige Werth (1) von K die Wurzel x der quadratischen Gleichung

$$Q_0 x^2-2P_0 x-Q_{-1}=0$$

darstellt, worin Q_{-1} den Werth (2) besitzt.

V. Um die nachfolgende Entwickelung nicht durch Nebenbemerkungen zu sehr zu stören, bemerken wir, dass die Wurzelgrösse, welche im Ausdrucke K im Zähler steht, zum Öfteren in den Nenner treten wird. Um einen solchen Ausdruck

auf die Form von K zu bringen, muss der Nenner rational gemacht werden. Dies geschieht allgemein nach der Formel

(3) $$\frac{M}{\sqrt{D}+N}=\frac{M(\sqrt{D}-N)}{(\sqrt{D}+N)(\sqrt{D}-N)}=\frac{M\sqrt{D}-MN}{D-N^2}$$

$$\text{oder} = \frac{\sqrt{D}+(-N)}{\frac{D-N^2}{M}}$$

VI. Es sei a^2 die grösste unterhalb D liegende Quadratzahl, wobei a nur als positiv gedacht wird, also

(4) $$D=a^2+b$$

worin b nicht $=0$ sein kann, sondern positiv >0 und $<2a+1$ ist, indem $(a+1)^2=a^2+2a+1$ sein würde. Hiernach ist

(5) $$\sqrt{D}=\sqrt{a^2+b}>a, \text{ aber } < a+1$$

Es wird mehrfach darauf ankommen, die grössten in einem Ausdrucke von der Form $\frac{\sqrt{D}+P}{Q}$ enthaltenen Ganzen oder den grössten Subquotienten dieses Ausdrucks zu bestimmen. Zu diesem Ende beachte man, dass wenn Q positiv ist, gleichviel welches Zeichen P hat,

(6) $$\frac{\sqrt{D}+P}{Q}>\frac{a+P}{Q}, \text{ aber} <\frac{a+1+P}{Q}$$

dass also, da $a+P$ eine ganze Zahl ist, die grössten Ganzen der irrationalen Grösse $\frac{\sqrt{D}+P}{Q}$ gleich den grössten Ganzen der rationalen Grösse $\frac{a+P}{Q}$ sind.

Denn wenn m die grössten Ganzen von $\frac{a+P}{Q}$, also $a+P$ $=mQ+R$ ist, worin R positiv und nicht grösser als $Q-1$ sein kann; so ist $a+1+P=mQ+R+1$ höchstens $=(m+1)Q$, also $\frac{a+1+P}{Q}$ höchstens $=m+1$. Da aber $\frac{\sqrt{D}+P}{Q}$ $<\frac{a+1+P}{Q}$ ist; so können die darin enthaltenen grössten Ganzen nur $=m$ sein.

Wäre dagegen Q negativ; so hätte man, gleichviel ob P positiv oder negativ ist,

(7) $$\frac{\sqrt{D}+P}{Q}>\frac{a+1+P}{Q}, \text{ aber} <\frac{a+P}{Q}$$

die gesuchten grössten Ganzen sind also dann die in dem Bruche $\frac{a+1+P}{Q}$ enthaltenen.

Bei den letzteren Bestimmungen des grössten Subquotienten hat man genau auf das Zeichen desselben zu achten (§. 10 und 18). Wenn also der Bruch $\frac{M}{N}$ positiv, z. B. $=\frac{19}{5}$; so ist der grösste Subquotient 3 auch der numerisch grösste Subquotient, welcher, wenn es sich um einen echten Bruch handelt, $=0$ wird. Ist dagegen der Bruch $\frac{M}{N}$ negativ, z. B. $=-\frac{19}{5}$; so ist der grösste Subquotient stets negativ und < 0, hier $=-4$, und seinem numerischen Werthe nach um Eine Einheit grösser, als der numerisch grösste Subquotient, insofern nicht schon $\frac{M}{N}$ genau eine ganze Zahl darstellt, welche dann der gesuchte grösste Subquotient selbst ist.

So hat man z. B. für $K=\frac{\sqrt{27}+6}{3}$, worin $D=5^2+2$ ist, $\frac{a+P}{Q}=\frac{5+6}{3}=\frac{11}{3}$, also $m=3$.

Für $K=\frac{\sqrt{27}-2}{1}$, $\frac{a+P}{Q}=\frac{5-2}{1}=\frac{3}{1}$, $m=3$.

Für $K=\frac{\sqrt{27}+6}{-3}$, $\frac{a+1+P}{Q}=\frac{5+1+6}{-3}=\frac{12}{-3}$, $m=-4$.

Für $K=\frac{\sqrt{27}-13}{-2}$, $\frac{a+1+P}{Q}=\frac{5+1-13}{-2}=\frac{7}{2}$, $m=3$.

Für $K=\frac{\sqrt{27}-20}{4}$, $\frac{a+P}{Q}=\frac{5-20}{4}=\frac{-15}{4}$, $m=-4$.

Für $K=\frac{\sqrt{27}+0}{9}$, $\frac{a+P}{Q}=\frac{5+0}{9}=\frac{5}{9}$, $m=0$.

Für $K=\frac{\sqrt{27}+0}{-9}$, $\frac{a+1+P}{Q}=\frac{5+1+0}{-9}=-\frac{6}{9}$, $m=-1$.

VII. Indem wir nun auf die Entwickelung der Grösse (1) in einen Kettenbruch näher eingehen, setzen wir, wenn a_0 der grösste Subquotient von $\frac{\sqrt{D}+P_0}{Q_0}$ ist,

$$K=x_0=\frac{\sqrt{D}+P_0}{Q_0}=a_0+\frac{1}{x_1} \tag{8}$$

Jenachdem K positiv und > 1, oder positiv und < 1, oder negativ ist, wird a_0 resp. positiv, oder null, oder negativ sein. Allein x_1 und alle ferner mit x_n zu bezeichnenden Grössen können nur positiv und >1 werden, und alle ferner mit a_p

zu bezeichnenden Quotienten können nur **positiv** und > 0 werden, wovon man sich durch das Nachfolgende überzeugen wird.

Lös't man Gl. (8) für x_1 auf; so kommt unter Berücksichtigung der in Gl. (3) angemerkten Transformation

$$x_1 = \frac{Q_0}{\sqrt{D} - a_0 Q_0 + P_0} = \frac{Q_0(\sqrt{D} + a_0 Q_0 - P_0)}{D - (a_0 Q_0 - P_0)^2}$$

$$= \frac{\sqrt{D} + a_0 Q_0 - P_0}{\frac{D - P_0^2}{Q_0} + 2 a_0 P_0 - a_0^2 Q_0}$$

Da nach Gl. (2) $\frac{D - P_0^2}{Q_0} = Q_{-1}$ eine ganze Zahl ist; so ist auch der Nenner des vorstehenden Werthes von x_1 eine ganze Zahl. Wir können also setzen

(9) $$x_1 = \frac{\sqrt{D} + a_0 Q_0 - P_0}{Q_{-1} + 2 a_0 P_0 - a_0^2 Q_0} = \frac{\sqrt{D} + P_1}{Q_1}, \text{ worin}$$

(10) $$P_1 = a_0 Q_0 - P_0$$

(11) $$Q_1 = \frac{D - P_1^2}{Q_0} = Q_{-1} + 2 a_0 P_0 - a_0^2 Q$$

VIII. Ist nun a_1 der grösste Subquotient von $\frac{\sqrt{D} + P_1}{Q_1}$; so setzen wir

$$x_1 = \frac{\sqrt{D} + P_1}{Q_1} = a_1 + \frac{1}{x_2}$$

Hieraus folgt durch Auflösung, wie vorhin

$$x_2 = \frac{Q_1}{\sqrt{D} - a_1 Q_1 + P_1} = \frac{Q_1(\sqrt{D} + a_1 Q_1 - P_1)}{D - (a_1 Q_1 - P_1)^2}$$

$$= \frac{\sqrt{D} + a_1 Q_1 - P_1}{\frac{D - P_1^2}{Q_1} + 2 a_1 P_1 - a_1^2 Q_1}$$

oder da nach Gl. (11) $\frac{D - P_1^2}{Q_1} = Q_0$ eine ganze Zahl ist,

(12) $$x_2 = \frac{\sqrt{D} + a_1 Q_1 - P_1}{Q_0 + 2 a_1 P_1 - a_1^2 Q_1} = \frac{\sqrt{D} + P_2}{Q_2}, \text{ worin}$$

(13) $$P_2 = a_1 Q_1 - P_1$$

(14) $$Q_2 = \frac{D - P_2^2}{Q_1} = Q_0 + 2 a_1 P_1 - a_1^2 Q_1$$

IX. Ist ferner a_2 der grösste Subquotient von $\frac{\sqrt{D} + P_2}{Q_2}$; so hat man in derselben Weise

$$x_2 = \frac{\sqrt{D} + P_2}{Q_2} = a_2 + \frac{1}{x_3} \text{ also}$$

$$x_3 = \frac{Q_2}{\sqrt{D} - a_2 Q_2 + P_2} = \frac{Q_2(\sqrt{D} + a_2 Q_2 - P_2)}{D - (a_2 Q_2 - P_2)^2}$$

$$= \frac{\sqrt{D} + a_2 Q_2 - P_2}{\frac{D - P_2^2}{Q_2} + 2 a_2 P_2 - a_2^2 Q_2}.$$

oder da nach Gl. (14) $\frac{D - P_2^2}{Q_2} = Q_1$ eine ganze Zahl ist,

(15) $$x_3 = \frac{\sqrt{D} + a_2 Q_2 - P_2}{Q_1 + 2 a_2 P_2 - a_2^2 Q_2} = \frac{\sqrt{D} + P_3}{Q_3},$$ worin

(16) $$P_3 = a_2 Q_2 - P_2$$

(17) $$Q_3 = \frac{D - P_3^2}{Q_2} = Q_1 + 2 a_2 P_2 - a_2^2 Q_2$$

X. Wenn allgemein a_n der grösste Subquotient von $\frac{\sqrt{D} + P_n}{Q_n}$ ist; so hat man

$$x_n = \frac{\sqrt{D} + P_n}{Q_n} = a_n + \frac{1}{x_{n+1}} \text{ also}$$

(18) $$x_{n+1} = \frac{Q_n}{\sqrt{D} - a_n Q_n + P_n} = \frac{Q_n(\sqrt{D} + a_n Q_n - P_n)}{D - (a_n Q_n - P_n)^2}$$

$$= \frac{\sqrt{D} + a_n Q_n - P_n}{\frac{D - P_n^2}{Q_n} + 2 a_n P_n - a_n^2 Q_n} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}},$$ worin

(19) $$P_{n+1} = a_n Q_n - P_n$$

(20) $$Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n} = Q_{n-1} + 2 a_n P_n - a_n^2 Q_n$$

XI. Diese Entwickelung, welche ohne Ende sein wird, kann man beliebig weit fortsetzen. Die Grössen a_0, a_1, a_2 . . . sind offenbar die Quotienten des gesuchten unendlichen Kettenbruchs, welcher $= K$ ist. Man hat also

(21) $$K = [a_0, a_1, a_2, a_3 \ldots]$$

worin a_0 positiv > 0, oder $= 0$ oder negativ < 0 ist, jenachdem K positiv > 1 oder positiv > 0 aber < 1, oder negativ ist, während alle übrigen Quotienten a_1, a_2 . . . nur positiv > 0 sein können.

Wenn man irgend Eine der mit x bezeichneten irrationalen Grössen, z. B. x_{n+1} wie den letzten Quotienten eines endlichen Kettenbruchs betrachtet; so hat man genau

(22) $$K = [a_0, a_1, a_2 \ldots a_n, x_{n+1}]$$

Es ist klar, dass wenn sich für irgend einen Zeiger n in der Grösse $x_n = \frac{\sqrt{D} + P_n}{Q_n}$ ganz genau die Grösse mit einem

früheren Zeiger m, also $x_m = \frac{\sqrt{D}+P_m}{Q_m}$ wiederholt, sodass $P_n = P_m$, $Q_n = Q_m$ ist, sich überhaupt in den Grössen von den Zeigern n, $n+1$, $n+2\ldots$ die früheren Grössen von den Zeigern m, $m+1$, $m+2\ldots$, dass sich also auch in den Quotienten a_n, a_{n+1}, $a_{n+2}\ldots$ die Quotienten a_m, a_{m+1}, $a_{m+2}\ldots$ wiederholen werden, sodass dann der fragliche Kettenbruch periodisch sein wird.

Es muss ausdrücklich darauf aufmerksam gemacht werden, dass der Gesammtwerth des durch vorstehende Entwickelung zum Vorschein kommenden unendlichen Kettenbruchs $[a_0, a_1, a_2\ldots]$ kein anderer sein kann, als der Werth der Grösse $K = \frac{\sqrt{D}+P_0}{Q_0}$, sodass eine Reduktion des ersteren genau die letztere Grösse wiedererzeugen muss. Diese Thatsache gründet sich aber darauf, dass wenn man jenen Kettenbruch bis zu irgend einem Quotienten a_n nimmt, man gegen den wahren Werth von K nur einen Fehler begeht, der darin besteht, dass statt des letzten Gliedes $x_n = a_n + \frac{1}{x_{n+1}}$ der Quotient a_n, also eine Grösse genommen ist, welche um keine volle positive Einheit kleiner ist, als x_n. Demnach müssen sich die sukzessiven Näherungswerthe des fraglichen Kettenbruches bis zu jedem Grade der Genauigkeit dem Werthe von K nähern, d. h. der Gesammtwerth des Kettenbruchs muss genau $= K$ sein.

§. 60. Beispiele.

Zur Erläuterung der im vorigen Paragraphen beschriebenen Rechnung mögen folgende Beispiele dienen. Wir schicken denselben die Bemerkung voraus, dass es zweckmässig ist, um die Entwickelung auf einen einfachen Mechanismus zurückzuführen, den Übergang von dem Gliede $\frac{\sqrt{D}+P_n}{Q_n}$ zu dem nächstfolgenden Gliede $\frac{\sqrt{D}+P_{n+1}}{Q_{n+1}}$ nach den beiden Formeln (19) und (20) des vorhergehenden Paragraphen zu bilden, also, nachdem man aus dem ersten Gliede den Quotienten a_n bestimmt hat, sofort den Werth von $a_n Q_n - P_n$ zu berechnen und als P_{n+1} zu notiren, hierauf den Werth von $\frac{D - P_{n+1}^2}{Q_n}$ zu berechnen und für Q_{n+1} zu nehmen.

Beispiel 1. $K = \frac{\sqrt{11}+9}{7}$, $D = 11 = 3^2 + 2$, $a = 3$, $Q_{-1} = \frac{11 - 9^2}{7} = -10$.

$$x_0 = \frac{\sqrt{11}+9}{7} = 1 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{11}-2}{1} = 1 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{11}+3}{2} = 3 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{11}+3}{1} = 6 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{11}+3}{2} = x_2$$
$$K = \frac{\sqrt{11}+9}{7} = [1, 1, \underbrace{3, 6}, \underbrace{3, 6} \ldots]$$

n	P_n	Q_n	a_n
-1		-10	
0	9	7	1
1	-2	1	1
2	3	2	3
3	3	1	6
4	3	2	3
5	3	1	6

Beispiel 2. $K = \frac{\sqrt{2}+5}{3} = \frac{\sqrt{18}+15}{9}$, $D = 18 = 4^2 + 2$, $a = 4$, $Q_{-1} = \frac{18 - 15^2}{9} = -23$.

$$x_0 = \frac{\sqrt{18}+15}{9} = 2 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{18}+3}{1} = 7 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{18}+4}{2} = 4 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{18}+4}{1} = 8 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{18}+4}{2} = x_2$$
$$K = \frac{\sqrt{2}+5}{3} = [2, 7, \underbrace{4, 8}, \underbrace{4, 8} \ldots]$$

n	P_n	Q_n	a_n
-1		-23	
0	15	9	2
1	3	1	7
2	4	2	4
3	4	1	8
4	4	2	4
5	4	1	8

Beispiel 3. $K = \frac{\sqrt{37}-4}{3}$, $D = 37 = 6^2 + 1$, $a = 1$, $Q_{-1} = \frac{37 - 4^2}{3} = 7$.

$$x_0 = \frac{\sqrt{37} - 4}{3} = 0 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{37} + 4}{7} = 1 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{37} + 3}{4} = 2 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{37} + 5}{3} = 3 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{37} + 4}{7} = x_1$$

n	P_n	Q_n	a_n
-1		7	
0	-4	3	0
1	4	7	1
2	3	4	2
3	5	3	3
4	4	7	1
5	3	4	2
6	5	3	3

$$K = \frac{\sqrt{37} - 4}{3} = [0, \underbrace{1, 2, 3,}\underbrace{1, 2, 3} \ldots]$$

Beispiel 4. $K = \frac{5 - \sqrt{2}}{2} = \frac{\sqrt{2} - 5}{-2} = \frac{\sqrt{8} - 10}{-4}$,

$D = 8 = 2^2 + 4,\ a = 2,\ Q_{-1} = \frac{8 - (-10)^2}{-4} = 23.$

$$x_0 = \frac{\sqrt{8} - 10}{-4} = 1 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{8} + 6}{7} = 1 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{8} + 1}{1} = 3 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{8} + 2}{4} = 1 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{8} + 2}{1} = 4 + \frac{1}{x_5}$$
$$x_5 = \frac{\sqrt{8} + 2}{4} = x_3$$

n	P_n	Q_n	a_n
-1		23	
0	-10	-4	1
1	6	7	1
2	1	1	3
3	2	4	1
4	2	1	4
5	2	4	1
6	2	1	4

$$K = \frac{5 - \sqrt{2}}{2} = [1, 1, 3, 1, 4, 4, 4 \ldots] .$$

Beispiel 5. $K = \sqrt{37} = \frac{\sqrt{37} + 0}{1}$, $D = 37 = 6^2 + 1$,
$a = 6,\ Q_{-1} = \frac{37 - 0^2}{1} = 37.$

$$x_0 = \frac{\sqrt{37} + 0}{1} = 6 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{37} + 6}{1} = 12 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{37} + 6}{1} = x_1$$

n	P_n	Q_n	a_n
-1		37	
0	0	1	6
1	6	1	12
2	6	1	12

$K = \sqrt{37} = [6, 12, 12, 12, \ldots]$

Beispiel 6. $K = \sqrt{29} = \frac{\sqrt{29}+0}{1}$, $D = 29 = 5^2 + 4$,

$a = 5$, $Q_{-1} = \frac{29 - 0^2}{1} = 29$.

$$x_0 = \frac{\sqrt{29}+0}{1} = 5 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{29}+5}{4} = 2 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{29}+3}{5} = 1 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{29}+2}{5} = 1 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{29}+3}{4} = 2 + \frac{1}{x_5}$$
$$x_5 = \frac{\sqrt{29}+5}{1} = 10 + \frac{1}{x_6}$$
$$x_6 = \frac{\sqrt{29}+5}{4} = x_1$$

n	P_n	Q_n	a_n
-1		29	
0	0	1	5
1	5	4	2
2	3	5	1
3	2	5	1
4	3	4	2
5	5	1	10
6	5	4	2
7	3	5	1
8	2	5	1
9	3	4	2
10	5	1	10

$K = \sqrt{29} = [5, \underbrace{2, 1, 1, 2, 10}, \underbrace{2, 1, 1, 2, 10} \ldots]$

Beispiel 7. $K = \sqrt{\tfrac{2}{3}} = \frac{\sqrt{6}+0}{3}$, $D = 6 = 2^2 + 2$,

$a = 2$, $Q_{-1} = \frac{6 - 0^2}{3} = 2$.

$$x_0 = \frac{\sqrt{6}+0}{3} = 0 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{6}+0}{2} = 1 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{6}+2}{1} = 4 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{6}+2}{2} = 2 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{6}+2}{1} = x_2$$

n	P_n	Q_n	a_n
-1		2	
0	0	3	0
1	0	2	1
2	2	1	4
3	2	2	2
4	2	1	4
5	2	2	2

$K = \sqrt{\tfrac{2}{3}} = [0, 1, 4, 2, 2, 2 \ldots]$

Beispiel 8. $K = \frac{\sqrt{2}-5}{3} = \frac{\sqrt{18}-15}{9}$, $D = 18 = 4^2 + 2$,

$a = 4$, $Q_{-1} = \frac{18 - (-15)^2}{9} = -23$.

$$x_0 = \frac{\sqrt{18}-15}{9} = -2 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{18}-3}{1} = 1 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{18}+4}{2} = 4 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{18}+4}{1} = 8 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{18}+4}{2} = x_2$$

n	P_n	Q_n	a_n
-1		-23	
0	-15	9	-2
1	-3	1	1
2	4	2	4
3	4	1	8
4	4	2	4
5	4	1	8

$$K = \frac{\sqrt{2}-5}{3} = [-2, 1, \underbrace{4, 8}, \underbrace{4, 8} \ldots]$$

Beispiel 9. $K = -\sqrt{3} = \frac{\sqrt{3}+0}{-1}$, $D = 3 = 1^2 + 2$, $a = 1$, $Q_{-1} = \frac{3-0^2}{-1} = -3$.

$$x_0 = \frac{\sqrt{3}+0}{-1} = -2 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{3}+2}{1} = 3 + \frac{1}{x_2}$$
$$x_2 = \frac{\sqrt{3}+1}{2} = 1 + \frac{1}{x_3}$$
$$x_3 = \frac{\sqrt{3}+1}{1} = 2 + \frac{1}{x_4}$$
$$x_4 = \frac{\sqrt{3}+1}{2} = x_2$$

n	P_n	Q_n	a_n
-1		-2	
0	0	-1	-2
1	2	1	3
2	1	2	1
3	1	1	2
4	1	2	1
5	1	1	2

$$K = -\sqrt{3} = [-2, 3, \underbrace{1, 2}, \underbrace{1, 2} \ldots]$$

§ 61. Beziehungen zwischen den Grössen P_n, Q_n, a_n und Nachweis der Periodizität derselben.

I. Zuvörderst wollen wir die aus §. 59 leicht sich ergebenden Beziehungen zwischen den Grössen P_n, Q_n, a_n übersichtlich zusammenstellen. Man hat P_0 und Q_0, sowie auch die Grösse $Q_{-1} = \frac{D - P_0^2}{Q_0}$ als gegeben zu betrachten. Die Grösse P_{-1} existirt nicht. Für die Grössen mit höhern Zeigern hat man

$$P_1 = a_0 Q_0 - P_0 \qquad Q_1 = \frac{D - P_1^2}{Q_0}$$
$$P_2 = a_1 Q_1 - P_1 \qquad Q_1 = \frac{D - P_2^2}{Q_1}$$

$$\vdots \qquad\qquad \vdots$$

(1) $P_n = a_{n-1} Q_{n-1} - P_{n-1}$ (3) $Q_n = \frac{D - P_n^2}{Q_{n-1}}$

(2) $P_{n+1} = a_n Q_n - P_n$ (4) $Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n}$

Dies sind die Grundformen für die Grössen P und Q. Ausserdem bestehen noch folgende von den vorstehenden abhängige bemerkenswerthe Beziehungen. Zuvörderst hat man nach §. 59

$$Q_1 = Q_{-1} + 2 a_0 P_0 - a_0^2 Q_0$$
$$Q_2 = Q_0 + 2 a_1 P_1 - a_1^2 Q_1$$
$$\vdots$$

(5) $Q_n = Q_{n-2} + 2 a_{n-1} P_{n-1} - a_{n-1}^2 Q_{n-1}$

(6) $Q_{n+1} = Q_{n-1} + 2 a_n P_n - a_n^2 Q_n$

Aus der Reihe (1), (2) ergeben sich die Gleichungen

$P_0 + P_1 = a_0 Q_0$ also auch $a_0 = \frac{P_0 + P_1}{Q_0}$

$P_1 + P_2 = a_1 Q_1$ $a_1 = \frac{P_1 + P_2}{Q_1}$

$$\vdots \qquad\qquad \vdots$$

(5^a) $P_{n-1} + P_n = a_{n-1} Q_{n-1}$ $a_{n-1} = \frac{P_{n-1} + P_n}{Q_{n-1}}$

(6^a) $P_n + P_{n+1} = a_n Q_n$ $a_n = \frac{P_n + P_{n+1}}{Q_n}$

Aus der Reihe (3), (4) ergeben sich die Gleichungen

$$Q_{-1} Q_0 = D - P_0^2$$
$$Q_0 Q_1 = D - P_1^2$$
$$Q_1 Q_2 = D - P_2^2$$
$$\vdots$$

(7) $Q_{n-1} Q_n = D - P_n^2$

(8) $Q_n Q_{n+1} = D - P_{n+1}^2$

Aus der Reihe (5), (6) ergeben sich unter Berücksichtigung der Reihe (1), (2) die Beziehungen

$Q_1 = Q_{-1} + a_0 (P_0 - P_1)$ oder $Q_1 - Q_{-1} = a_0 (P_0 - P_1)$

$Q_2 = Q_0 + a_1 (P_1 - P_2)$ $Q_2 - Q_0 = a_1 (P_1 - P_2)$

$$\vdots \qquad\qquad \vdots$$

(9) $Q_n = Q_{n-2} + a_{n-1} (P_{n-1} - P_n)$

(10) $Q_{n+1} = Q_{n-1} + a_n (P_n - P_{n+1})$

oder

(11) $$Q_n - Q_{n-2} = a_{n-1}(P_{n-1} - P_n)$$
(12) $$Q_{n+1} - Q_{n-1} = a_n(P_n - P_{n+1})$$

Es ist klar, dass sowol die Reihe (3), (4), wie auch die Reihe (9), (10) als Rekursionsformeln zur Berechnung der Grössen Q unter gleichzeitiger Benutzung der Reihe (1), (2) als Rekursionsformeln zur Berechnung der Grössen P verwendet werden kann, wenn man zu gleicher Zeit die Quotienten a_n bildet. Was die Lètzteren betrifft; so hat man zunächst für die irrationalen Brüche x_n

$$x_0 = \frac{\sqrt{D} + P_0}{Q_0} = a_0 + \frac{1}{x_1}$$
$$x_1 = \frac{\sqrt{D} + P_1}{Q_1} = a_1 + \frac{1}{x_2}$$
$$\vdots$$
(13) $$x_n = \frac{\sqrt{D} + P_n}{Q_n} = a_n + \frac{1}{x_{n+1}}$$
(14) $$x_{n+1} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}} = a_{n+1} + \frac{1}{x_{n+2}}$$

worin die Grössen x vom Zeiger 1 an, also $x_1, x_2, \ldots$ sämmtlich positiv und > 1, also $\frac{1}{x_1}, \frac{1}{x_2} \ldots$ sämmtlich positiv und $> 0, < 1$ sind.

II. Wenn $D = a^2 + b$ gesetzt wird, sodass a^2 die grösste unterhalb D liegende Quadratzahl ist; so ist der Quotient a_n auch der grösste Subquotient des rationalen Bruches $\frac{a + P_n}{Q_n}$, insofern Q_n positiv ist, dagegen des rationalen Bruches $\frac{a + 1 + P_n}{Q_n}$, insofern Q_n negativ ist. Man hat also, wenn man den Rest der Division mit Q_n in den Zähler dieses rationalen Bruches mit R_n und jenen Bruch selbst mit y_n bezeichnet, wenn Q_n positiv ist

(15) $y_n = \frac{a + P_n}{Q_n} = a_n + \frac{R_n}{Q_n}$ also (16) $a + P_n = a_n Q_n + R_n$

und wenn Q_n negativ ist,

(17) $y_n = \frac{a + 1 + P_n}{Q_n} = a_n + \frac{R_n}{Q_n}$ also (18) $a + 1 + P_n = a_n Q_n + R_n$

In beiden Fällen ist der Bruch $\frac{R_n}{Q_n}$ positiv und < 1, also R_n in Gl. (15) und (16) positiv und $< Q_n$, aber in Gl. (17) und (18) negativ und numerisch $< Q_n$. Unter Umständen kann $R_n = 0$ sein; sonst hat diese Grösse immer dasselbe Zeichen wie Q_n.

Bezeichnen wir nun augenblicklich mit P_n, Q_n und R_n nur entschieden positive Grössen; so kann irgend ein irrationaler Bruch x_n, dessen Zeiger $n > 0$ ist, da derselbe durchaus positiv sein muss (§. 59), nur in Einer der drei nachstehenden Formen erscheinen

$$\left.\begin{aligned} &(19) \quad x_n = \frac{\sqrt{D} + P_n}{Q_n} \\ &(20) \quad x_n = \frac{\sqrt{D} - P_n}{Q_n} \\ &(21) \quad x_n = \frac{\sqrt{D} - P_n}{-Q_n} \end{aligned}\right\} = a_n + \frac{1}{x_{n+1}}$$

Der betreffende rationale Bruch y_n, aus welchem der grösste Subquotient a_n bestimmt wird, ist dann resp.

$$\left.\begin{aligned} &(22) \quad y_n = \frac{a + P_n}{Q_n} \\ &(23) \quad y_n = \frac{a - P_n}{Q_n} \\ &(24) \quad y_n = \frac{a + 1 - P_n}{-Q_n} \end{aligned}\right\} = a_n + \frac{R_n}{Q_n}$$

III. Erster Fall (19), (22). In diesem Falle erscheint nach Gl. (19) die auf x_n folgende Grösse x_{n+1} in der Gestalt

$$(25) \qquad x_{n+1} = \frac{\sqrt{D} + (a_n Q_n - P_n)}{\dfrac{D - (a_n Q_n - P_n)^2}{Q_n}} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}}$$

Nach Gl. (22) hat man $a + P_n = a_n Q_n + R_n$ also

$$(26) \qquad P_{n+1} = a_n Q_n - P_n = a - R_n$$

Da $R_n < Q_n$; so ist $a_n Q_n + R_n > (a_n + 1) R_n$ also

$$(27) \qquad a + P_n > (a_n + 1) R_n \text{ oder } R_n < \frac{a + P_n}{a_n + 1}$$

Ist nun $P_n \leqq a$; so ist nach (27) $R_n < a$ (oder auch $= a$, was jedoch nur dann eintreten kann, wenn $P_n = a$ und $a_n = 1$ ist) und folglich ist nach (26) P_{n+1} positiv und $\leqq a$. Ferner ist alsdann, weil x_{n+1} positiv sein muss, nach (25) Q_{n+1} positiv.

Ist $P_n > a$, aber $< a_n Q_n$; so ist nach (26) ebenfalls P_{n+1} positiv und $\leqq a$, und folglich nach (25) Q_{n+1} positiv.

Ist $P_n > a$ und $\geqq a_n Q_n$; so leuchtet aus (26) ein, dass $P_n - a_n Q_n = R_n - a$ positiv (resp. null), also $R_n \geqq a$ und demnach entschieden $Q_n > a$ sein muss. Die Voraussetzung ist also nur möglich, wenn $Q_n > a$ ist. Ausserdem folgt aus (26), dass P_{n+1} negativ (resp. $= 0$) werden wird, und man erhält, da x_{n+1} positiv sein muss, entweder die Form

$$x_{n+1} = \frac{\sqrt{D} - P_{n+1}}{Q_{n+1}}, \text{ worin } P_{n+1} < a \text{ ist,}$$

oder die Form

$$x_{n+1} = \frac{\sqrt{D} - P_{n+1}}{-Q_{n+1}}, \text{ worin } P_{n+1} > a \text{ ist.}$$

In der letzten Form ist aber der absolute Werth $P_n - a_n Q_n$ von $P_{n+1} < P_n$.

IV. Zweiter Fall (20), (23). In diesem Falle muss nothwendig, damit x_n positiv sein könne, $P_n \leqq a$ sein. Man hat dann x_{n+1} in der Form

$$(28) \qquad x_{n+1} = \frac{\sqrt{D} + (a_n Q_n + P_n)}{\frac{D - (a_n Q_n + P_n)^2}{Q_n}} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}}$$

Nach (23) hat man $a - P_n = a_n Q_n + R_n$ also

$$(29) \qquad P_{n+1} = a_n Q_n + P_n = a - R_n$$

Es ist also P_{n+1} positiv und $\leqq a$. Ferner ist Q_{n+1}, weil x_{n+1} positiv sein muss, ebenfalls positiv.

Es ist wichtig, dass die letzteren Behauptungen für P_{n+1} und Q_{n+1} auch dann Gültigkeit haben, wenn $P_n > a$, also x_n und a_n negativ sein sollten, insofern $Q_n \leqq a$ ist. Denn es ist alsdann $R_n < Q_n$, folglich auch $< a$, mithin $P_{n+1} = a - R_n$ positiv und $\leqq a$ und demnach Q_{n+1} positiv. Dieser Fall kann sich übrigens nur für den Zeiger $n = 0$ ereignen.

V. Dritter Fall (21), (24). In diesem Falle muss, damit x_n positiv sein könne, $P_n > a$ sein. Man hat dann x_{n+1} in der Form

$$(30) \qquad x_{n+1} = \frac{\sqrt{D} + (P_n - a_n Q_n)}{\frac{D - (P_n - a_n Q_n)^2}{-Q_n}} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}}$$

Nach (24) ist $a + 1 - P_n = -a_n Q_n - R_n$ also

$$(31) \qquad P_{n+1} = P_n - a_n Q_n = a + 1 + R_n$$

Demnach ist P_{n+1} positiv und $> a$, aber gleichwol $< P_n$. Ausserdem ist Q_{n+1}, weil x_{n+1} positiv sein muss, positiv.

VI. Aus dem Vorstehenden ergibt sich folgendes Gesetz.

Wenn irgend ein P grösser als a ist; so muss der absolute Betrag des nächstfolgenden P, wenn derselbe nicht kleiner oder gleich a wird, doch durchaus kleiner, als der Betrag des vorhergehenden P werden. Unter diesen Umständen können sich wol in den späteren Stellen einigemal negative Werthe von P und Q ergeben; sobald jedoch an irgend einer Stelle $P \leqq a$ geworden ist, was unter jenen Umständen doch endlich einmal geschehen muss; so bleibt in allen folgenden Stellen sowol P, als auch Q positiv und zugleich $P \leqq a$, mithin wegen Gl. (22) $Q \leqq a + P$ und noch weit mehr $Q \leqq 2a$.

Nachdem dieser letztere Zustand erreicht ist, was in einigen der vorhin erörterten Fälle schon von vorn herein geschieht,

und in den übrigen endlich einmal geschehen wird, müssen sich an irgend einer späteren Stelle zwei zusammengehörige Werthe von P und Q wiederholen. Es kann sich jedoch von dort an niemals ein früherer negativer Werth von P oder Q, auch kein positiver Werth von P, welcher grösser als a wäre, wiederholen.

Hieraus folgt, dass von einer gewissen Stelle an die Grössen P und Q Perioden bilden werden, in denen nur positive Werthe, und zwar für $P \leqq a$ und für $Q \leqq 2a$ erscheinen können. Ferner ergibt sich hieraus, dass auch die Quotienten a_n des Kettenbruches K von derselben Stelle an gleich lange Perioden bilden werden, in denen nur positive Zahlen auftreten können, welche nicht kleiner als 1 und nach Gl. (22) nicht grösser als $2a$ sind.

VII. Endlich ist wegen der Beziehung $Q_{n-1} Q_n = D - P_n^2$ klar, dass wenn P_n, Q_n, a_n die ersten Grössen sind, welche sich für einen späteren Zeiger wiederholen, auch die Grösse Q_{n-1} vom nächstvorhergehenden Zeiger sich wiederholen muss, sodass, wenn man die Reihen der Grössen P_n, Q_n, a_n abgesondert von einander betrachtet, die Periode der Q um Einen Zeiger früher beginnt, als die Periode der P und die der Quotienten.

Demnach kann man die Gesammtperiode der drei Grössen P_n, Q_n, a_n von den Einzelperioden dieser Grössen unterscheiden.

§. 62. *Anfang der Periode.*

I. Für die Untersuchungen über die Periodizität der Grössen P_n, Q_n, a_n sind noch folgende Beziehungen von Wichtigkeit.

Wenn für den Zeiger n in dem Ausdrucke $x_n = \dfrac{\sqrt{D} + P_n}{Q_n}$ die Grössen P_n und Q_n positiv sind und folgenden drei Bedingungen

(1) $Q_n \leqq a + P_n$ oder $Q_n < \sqrt{D} + P_n$ oder $x_n > 1$

(2) $P_n \leqq a$ » $P_n < \sqrt{D}$

(3) $P_n + Q_n \geqq a + 1$ » $P_n + Q_n > \sqrt{D}$

entsprechen; so erfüllen auch alle Grössen von den späteren Zeigern $n+1$, $n+2\ldots$ dieselben Bedingungen. Für die Bedingungen (1) und (2) ist Dies schon im vorhergehenden Paragraphen nachgewiesen, und es muss bemerkt werden, dass wenn Q_n positiv ist, die Bedingung (1) für jeden Zeiger n, welcher > 0 ist, erfüllt sein wird.

Was die Bedingung (3) betrifft; so lehrt die bekannte Beziehung $P_{n+1} = a_n Q_n - P_n$, woraus $P_n + P_{n+1} = a_n Q_n$ folgt, dass

(4) $$P_n + P_{n+1} \geqq Q_n$$

ist. Da nun $Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n}$ ist; so hat man

$$P_{n+1} + Q_{n+1} = P_{n+1} + \frac{D - P_{n+1}^2}{Q_n} \geqq P_{n+1} + \frac{D - P_{n+1}^2}{P_n + P_{n+1}}$$

oder wenn man $D = a^2 + b$ setzt, nach gehöriger Transformation

$$P_{n+1} + Q_{n+1} \geqq a + \frac{(a - P_n)(a - P_{n+1}) + b}{P_n + P_{n+1}}$$

Da $a - P_n$ und $a - P_{n+1}$ positiv und mindestens $= 0$ sind, b aber nicht kleiner als 1 sein kann; so folgt

$$P_{n+1} + Q_{n+1} \geqq a + 1 \text{ oder } > \sqrt{D}$$

was zu beweisen war.

Um zu diesem Schlusse zu gelangen, bedurfte es nur der Existenz der beiden Bedingungen (1) und (2). Diese beiden, welche nach §. 61 endlich einmal eintreten müssen, ziehen also die dritte Bedingung (3) als eine nothwendige Konsequenz für alle späteren Zeiger nach sich.

Man kann demnach auch sagen, wenn die beiden Bedingungen (1) und (2) für den Zeiger n bestehen; so gelten die drei Bedingungen (1), (2), (3) für den Zeiger $n+1$ und für alle späteren.

Wir notiren hier auch noch die aus $\frac{a + P_n}{Q_n} < a_n + 1$ sich ergebende Beziehung $a + P_n < a_n Q_n + Q_n$ oder

$$Q_n + a_n Q_n - P_n > a \text{ oder } \geqq a + 1, \text{ d. i.}$$

(5) $$Q_n + P_{n+1} \geqq a + 1 \text{ oder } > \sqrt{D}$$

II. Was nun den Anfang der Periode betrifft; so folgt aus dem Vorstehenden, dass es einen in den Perioden liegenden Zeiger m geben muss, für welchen sich in dem späteren Zeiger n die Grössen P_m, Q_m, a_m dergestalt wiederholen, dass nun auch alle folgenden Grössen von den Zeigern $m+1$, $m+2$... mit denen von den Zeigern $n+1$, $n+2$... übereinstimmen, während für alle diese Grössen die drei Bedingungen (1), (2), (3) erfüllt sind. Hieraus erhellet, dass für alle in den Perioden liegenden Grössen jene drei Bedingungen erfüllt sein müssen. Auch muss $Q_{m-1} = Q_{n-1}$ sein.

Gehen wir nun rückwärts, um die Grössen P_{m-1}, a_{m-1} mit P_{n-1}, a_{n-1} zu vergleichen; so erhalten wir durch Subtraktion der bekannten Beziehungen

$$P_m = a_{m-1} Q_{m-1} - P_{m-1}$$
$$P_n = a_{n-1} Q_{n-1} - P_{n-1}$$
$$P_m - P_n = a_{m-1} Q_{m-1} - a_{n-1} Q_{n-1} - P_{m-1} + P_{n-1}$$

oder da $P_m = P_n$, $Q_{m-1} = Q_{n-1}$ ist,

(6) $$P_{m-1} - P_{n-1} = (a_{m-1} - a_{n-1})\, Q_{n-1}$$

Wenn nun Q_{n-1} positiv, also auch, insofern $n-1 > 0$, die Bedingung (1) erfüllt ist; so ist klar, dass jenachdem $P_{m-1} >, <, = P_{n-1}$ ist, auch $a_{m-1} >, <, = a_{n-1}$ sein muss. Wäre aber $P_{m-1} > P_{n-1}$, also auch $a_{m-1} > a_{n-1}$; so hätte man

$$P_{m-1} = P_{n-1} + (a_{m-1} - a_{n-1})\, Q_{n-1} \geqq P_{n-1} + Q_{n-1}$$

also, da P_{n-1} und Q_{n-1} in der Periode liegen, nach (5) entschieden

$$P_{m-1} > a$$

Ist nun aber für den Zeiger $m-1$ die Bedingung (2) erfüllt; so ist das vorstehende Resultat unmöglich.

Wäre dagegen $P_{m-1} < P_{n-1}$, also auch $a_{m-1} < a_{n-1}$; so ergibt eine Umkehrung der Gl. (6), wenn man auch Q_{m-1} für Q_{n-1} schreibt,

$$P_{n-1} = P_{m-1} + (a_{n-1} - a_{m-1})\, Q_{m-1} \geqq P_{m-1} + Q_{m-1}$$

Ist nun aber für den Zeiger $m-1$ die Bedingung (3) erfüllt, also $P_{m-1} + Q_{m-1} > a$; so ist das vorstehende Resultat unmöglich, weil das in der Periode liegende $P_{n-1} < a$ sein muss.

Wenn also die drei Bedingungen (1), (2), (3) auch für den Zeiger $m-1$ gelten; so kann P_{m-1} weder $>$, noch $< P_{n-1}$ sein, muss vielmehr $= P_{n-1}$ sein. Demnach muss auch $a_{m-1} = a_{n-1}$ sein, und man sieht, dass für diese Voraussetzung P_{m-1}, Q_{m-1}, a_{m-1} resp. $= P_{n-1}$, Q_{n-1}, a_{n-1}, also auch $Q_{m-2} = Q_{n-2}$ ist.

Aus Vorstehendem folgt, dass sich alle diejenigen Grössen von den unterhalb m liegenden Zeigern $m-1$, $m-2\ldots$ wiederholt haben müssen, für welche die Bedingungen (1), (2), (3) erfüllt sind.

Da nun nachgewiesen ist, dass die Erfüllung der Bedingungen (1), (2), (3) für irgend einen Zeiger ihren Fortbestand für alle folgenden Zeiger nach sich zieht, ferner, dass alle in den Perioden liegenden Grössen den eben genannten Bedingungen entsprechen müssen, endlich, dass die Perioden rückwärts sich soweit fortsetzen müssen, als jene Bedingungen erfüllt sind; so leuchtet ein, dass diese Bedingungen für die in der Gesammt-Periode liegenden Grössen ausschliesslich charakteristisch sind, und dass die erste Periode mit dem niedrigsten Zeiger beginnt, für welchen jene Bedingungen sich verwirklichen.

Man kann auch sagen, dass die beiden Bedingungen (1) und (2) charakteristisch sind für ein Glied, auf welches nothwendig ein zur Periode gehöriges Glied folgen muss.

III. Anfang der Periode für spezielle Fälle. — Wenn in dem gegebenen Ausdrucke $K = \frac{\sqrt{D} + P_0}{Q_0}$ $P_0 = 0$ und Q_0 positiv ist, also für Ausdrücke wie $\sqrt{D}$ und $\frac{\sqrt{D}}{Q_0}$, kön-

nen die beiden Bedingungen (1) und (3) für den Zeiger $n=0$ nicht gleichzeitig erfüllt sein, indem man hiernach $Q_0 < \sqrt{D}$ und $Q_0 > \sqrt{D}$ haben müsste, was unmöglich ist.

Die Periode kann also in diesen Fällen niemals mit dem Zeiger 0 beginnen.

Es wird aber für den nächstfolgenden Zeiger 1 jedenfalls die Bedingung (1), nämlich $Q_1 < \sqrt{D} + P_1$, sowie auch die Bedingung (2), nämlich $P_1 < \sqrt{D}$ erfüllt sein (§. 61). Was die Bedingung (3) oder $P_1 + Q_1 > \sqrt{D}$ betrifft; so hat man $P_1 = a_0 Q_0$, $Q_1 = \frac{D - a_0^2 Q_0^2}{Q_0}$, und die fragliche Bedingung verlangt

$$a_0 Q_0 + \frac{D - a_0^2 Q_0^2}{Q_0} > \sqrt{D}$$

oder nach gehöriger Reduktion

$$\frac{\sqrt{D}}{Q_0}\left(\frac{\sqrt{D}}{Q_0} - 1\right) > a_0 (a_0 - 1) \text{ oder}$$

$$K(K-1) > a_0 (a_0 - 1)$$

Diese Bedingung ist erfüllt, wenn $K = \frac{\sqrt{D}}{Q_0}$ ein unechter Bruch, also $a_0 \geqq 1$ ist. Unter solchen Umständen beginnt also die Periode mit dem Zeiger 1. Z. B.

$$K = \frac{\sqrt{24}}{3} = [1, \underbrace{1, 1, 1, 2,} \underbrace{1, 1, 1, 2,} \ldots]$$

Jene Bedingung ist jedoch nicht erfüllt, wenn $K = \frac{\sqrt{D}}{Q_0}$ ein echter Bruch, also $a_0 = 0$ ist, indem man alsdann $P_1 + Q_1 = \frac{D}{Q_0} < \sqrt{D}$ hat, indem aus $\frac{\sqrt{D}}{Q_0} < 1$ nothwendig $\frac{\sqrt{D}.\sqrt{D}}{Q_0} = \frac{D}{Q_0} < \sqrt{D}$ folgt. Unter solchen Umständen ist übrigens $x_1 = \frac{\sqrt{D} + P_1}{Q_1} = \frac{\sqrt{D} + 0}{\frac{D}{Q_0}} = \frac{Q_0}{\sqrt{D}} = \frac{1}{K} > 1$. Es muss also nach dem vorhergehenden Satze die Periode der Grössen x mit dem zweiten Zeiger, also die Periode von K mit dem dritten Zeiger, d. h. mit dem Zeiger 2 beginnen. Z. B.

$$K = \frac{\sqrt{24}}{8} = [0, 1, \underbrace{1, 1, 1, 2,} \underbrace{1, 1, 1, 2} \ldots]$$

Die in Rede stehenden drei Bedingungen können schon für

den Zeiger 0 in dem gegebenen Werthe $K = \frac{\sqrt{D} + P_0}{Q_0}$ erfüllt sein, in welchem Falle jedoch, wie gezeigt ist, P_0 nicht $= 0$ sein kann. Unter solchen Umständen beginnt die Periode mit dem Zeiger 0. Z. B.

$$K = \frac{\sqrt{18} + 4}{2} = [\underbrace{4, 8,}\underbrace{4, 8,}\underbrace{4, 8,}\ldots]$$

§. 63. **Schluss der Periode.**

I. Wenn m der Zeiger unmittelbar vor der ersten Periode, $m+1$ der erste Zeiger und n der letzte Zeiger in dieser Periode ist, sodass alle Grössen von den Zeigern $m+1$, $m+2\ldots$ resp. mit denen von den Zeigern $n+1$, $n+2\ldots$ übereinstimmen; so hat man immer auch für das letzte Q in der Periode

(1) $$Q_n = Q_m$$

Was den Werth des letzten P in der Periode betrifft; so ist

$$P_n + Q_n = P_n + Q_m > a \text{ also}$$

(2) $P_n > a - Q_m$. Ausserdem ist aber auch

(3) $P_n \leqq a$

Um für den letzten Quotienten a_n in der Periode eine Beziehung zu erhalten, beachten wir, dass nach §. 61 Gl. (16) $a = a_m Q_m - P_m + R_m$ ist. Hierdurch werden die vorstehenden beiden Ungleichheiten resp.

$$P_n > a_m Q_m - P_m + R_m - Q_m$$
$$P_n \leqq a_m Q_m - P_m + R_m$$

Nun ist aber, wie im vorhergehenden Paragraphen Gl. (6)

$$P_n = P_m + (a_n - a_m) Q_m = a_n Q_m - (a_m Q_m - P_m)$$

Substituirt man diesen Werth für P_n in die vorstehenden beiden Ungleichheiten; so kommt

$$a_n Q_m - (a_m Q_m - P_m) \begin{cases} > a_m Q_m - P_m + R_m - Q_m \\ \leqq a_m Q_m - P_m + R_m \end{cases}$$

Hieraus folgt

(4) $$a_n > 2 a_m - \frac{2 P_m}{Q_m} + \frac{R_m}{Q_m} - 1$$

(5) $$a_n \leqq 2 a_m - \frac{2 P_m}{Q_m} + \frac{R_m}{Q_m}$$

Zwischen diesen beiden Gränzen, deren Differenz < 1 ist, liegt nur eine einzige ganze Zahl, welche $= a_n$ ist.

Wenn $2 P_m$ ein genaues Vielfaches von Q_m, also $\frac{2 P_m}{Q_m}$ eine ganze Zahl c ist; so kann offenbar nur

(6) $$a_n = 2 a_m - \frac{2 P_m}{Q_m} = 2 a_m - c$$

sein. Diesen Ausdruck kann man auch, da $a_m Q_m - P_m = P_{m+1}$ ist, in die Form

(7) $$a_n = \frac{2P_{m+1}}{Q_m}$$

bringen, woraus folgt, dass wenn $\frac{2P_m}{Q_m}$ eine ganze Zahl ist, auch $\frac{2P_{m+1}}{Q_m}$ eine solche sein wird.

II. Schluss der Periode für spezielle Fälle. Für die ersten beiden im vorhergehenden Paragraphen erwähnten speziellen Fälle $K = \sqrt{D}$ und $K = \frac{\sqrt{D}}{Q_0} > 1$ beginnt die Periode mit dem Zeiger $m+1=1$. Man hat also $m=0$, und da $P_m = P_0 = 0$, folglich $\frac{2P_m}{Q_m} = \frac{2.0}{Q_0} = c = 0$ ist; so schliesst die Periode der Quotienten mit $a_n = 2a_m = 2a_0$.

Für den dritten dort erwähnten speziellen Fall $K = \frac{\sqrt{D}}{Q_0} < 1$ beginnt die Periode mit dem Zeiger $m+1=2$. Man hat also $m=1$, und da $P_m = P_1 = 0$, folglich ebenfalls $\frac{2P_m}{Q_m} = 0$ ist; so schliesst die Periode der Quotienten mit $a_n = 2a_m = 2a_1$.

In allen Fällen also, wo $P_0 = 0$ ist, besitzt der letzte Quotient der Periode den doppelten Werth des der ersten Periode vorhergehenden Quotienten.

Bei der Entwickelung einer reinen Quadratwurzel $K = \sqrt{D}$ geht mithin der ersten Periode der Quotient a_0 voran, welcher gleich den grössten in $\sqrt{D}$ enthaltenen Ganzen, d. i. $= a$ ist, und jede Periode schliesst mit dem Doppelten dieser Zahl, also mit $2a$.

§. 64. Symmetrie der Periode.

I. Wenn nach der Bezeichnung des vorhergehenden Paragraphen $\frac{2P_m}{Q_m}$ eine ganze Zahl c ist; so besteht unter den in der Periode liegenden Grössen ein bemerkenswerthes Gesetz. Man hat nämlich zuvörderst nach §. 63 Gl. (7)

$$a_n\, Q_m = 2P_{m+1}$$

und da nach jenem Paragraphen auch

$$P_n = a_n\, Q_m - (a_m\, Q_m - P_m) = a_n\, Q_m - P_{m+1}$$

ist; so hat man

(1) $$P_n = P_{m+1} = P_{n+1}$$

d. h. unter solchen Umständen ist das letzte P der Periode gleich dem ersten der Periode.

Hiernach folgt sofort aus der Gl. (10) des §. 61

(2) $$Q_{n-1} = Q_{n+1} = Q_{m+1}$$

Subtrahirt man den Werth für P_n von dem für P_{n+2} aus der Reihe (1), (2) des §. 61; so kommt unter Berücksichtigung, dass $P_n = P_{n+1}$ und $Q_{n-1} = Q_{n+1}$ ist,

$$P_{n+2} - P_{n-1} = (a_{n+1} - a_{n-1})\ Q_{n-1}$$

Wäre nun $P_{n+2} > P_{n-1}$ und mithin gleichzeitig $a_{n+1} > a_{n-1}$; so hätte man wegen §. 62, (3)

$$P_{n+2} = P_{n-1} + (a_{n+1} - a_{n-1})\ Q_{n-1} \geqq P_{n-1} + Q_{n-1} > a$$

was wegen §. 62, (2) unmöglich ist.

Wäre aber $P_{n+2} < P_{n-1}$, also auch $a_{n+1} < a_{n-1}$; so hätte man durch Umkehrung der Gleichung und Substitution von Q_{n+1} für Q_{n-1}

$$P_{n-1} = P_{n+2} + (a_{n-1} - a_{n+1})\ Q_{n+1}$$

Substituirt man auf der rechten Seite $Q_{n+1} = \frac{D - P_{n+2}^2}{Q_{n+2}}$ $= \frac{a^2 + b - P_{n+2}^2}{Q_{n+2}} = \frac{(a + P_{n+2})\ (a - P_{n+2}) + b}{Q_{n+2}}$; so kann man die vorstehende Gleichung in folgende Form bringen

$$P_{n-1} = a + \frac{[(a_{n-1} - a_{n+1})\ (a + P_{n+2}) - Q_{n+2}]\ (a - P_{n+2}) + (a_{n-1} - a_{n+1}) b}{Q_{n+2}}$$

Da $a_{n-1} + a_{n+1} \geqq 1$ und nach §. 62, (1) $a + P_{n+2} \geqq Q_{n+2}$ ist; so würde entschieden $P_{n-1} > a$ sein, was nach §. 62, (2) unmöglich ist.

Demnach kann nur sein

(3) $\qquad a_{n-1} = a_{n+1} = a_{m+1}$ und

(4) $\qquad P_{n-1} = P_{n+2} = P_{m+2}$

Um jetzt weiter zu schliessen, subtrahirt man immer zuerst diejenigen beiden Gleichungen aus der Reihe (7), (8) des §. 61, in welchen die beiden zuletzt als gleich gefundenen Werthe von P, d. i. jetzt P_{n-1} und P_{n+2} vorkommen, indem man dabei die Gleichung der zuletzt als gleich gefundenen Werthe von Q, d. i. jetzt $Q_{n-1} = Q_{n+1}$ berücksichtigt. Dies gibt zunächst

(5) $\qquad Q_{n-2} = Q_{n+2} = Q_{m+2}$

Hierauf subtrahirt man diejenigen beiden Gleichungen aus der Reihe (1), (2) des §. 61, in deren erster auf der linken Seite das niedrigere der beiden zuletzt als gleich befundenen P, also jetzt P_{n-1} vorkommt, während in der zweiten auf der rechten Seite das höhere jener beiden P, also jetzt P_{n+2} vorkommt, indem man dabei die Gleichheit aller bis dahin als gleich befundenen Q berücksichtigt. Dies gibt nach einem dem vorstehenden ganz ähnlichen Schlussverfahren zunächst

(6) $\qquad a_{n-2} = a_{n+2} = a_{m+2}$

(7) $\qquad P_{n-2} = P_{n+3} = P_{m+3}$

Aus Vorstehendem folgt, dass wenn $\frac{2 P_m}{Q_m} = c$ eine ganze Zahl ist, die Periode, welche sich für alle in Rede stehenden

Grössen vom Zeiger $m+1$ bis zum Zeiger n erstreckt, für die Grössen P zwischen den Gliedern P_{m+1} und P_n, für die Grössen Q zwischen den Gliedern Q_{m+1} und Q_{n-1} und für die Quotienten zwischen den Gliedern a_{m+1} und a_{n-1} von beiden Enden her gleiche Werthe enthält, während man für das letzte ausserhalb dieser symmetrischen Reihenfolge liegende Glied der Grössen Q $Q_n = Q_m$ und der Quotienten $a_n = 2a_m - c$ hat. Eine Periode von dieser Art wird symmetrisch genannt. Das Schema einer symmetrischen Periode ist hiernach folgendes:

							1. symm. Periode					2. symm. P.		
	0	1	2	...	m−1	m	m+1	m+2	...	n−1	n	n+1	n+2	...
	P_0	P_1	P_2	...	P_{m-1}	P_m	P_{m+1}	P_{m+2}	...	P_{m+2}	P_{m+1}	P_{m+1}	P_{m+2}	...
Q_{-1}	Q_0	Q_1	Q_2	...	Q_{m-1}	Q_m	Q_{m+1}	Q_{m+2}	...	Q_{m+1}	Q_m	Q_{m+1}	Q_{m+2}	...
	a_0	a_1	a_2	...	a_{m-1}	a_m	a_{m+1}	a_{m+2}	...	a_{m+1}	$2a_m-c$	a_{m+1}	a_{m+2}	...

II. Nach Obigem ergibt sich aus der Voraussetzung, dass $\frac{2P_m}{Q_m}$ eine ganze Zahl sei, die Symmetrie der Periode; umgekehrt erfordert aber auch diese Symmetrie, dass $\frac{2P_m}{Q_m}$ eine ganze Zahl sei. Denn wenn $P_n = P_{m+1}$, $Q_n = Q_m$ und $Q_{n-1} = Q_{n+1}$ sein soll; so muss nach §. 61 Gl. (6) $0 = 2a_n P_{m+1} - a_n^2 Q_m$ also $a_n = \frac{2P_{m+1}}{Q_m}$ $= \frac{2(a_m Q_m - P_m)}{Q_m} = 2a_m - \frac{2P_m}{Q_m}$ sein.

Dann also, aber auch nur dann, wenn unter den Grössen P_m, Q_m zwei solche vorkommen, für welche $\frac{2P_m}{Q_m}$ eine ganze Zahl ist, bilden die fraglichen Grössen vom Zeiger $m+1$ an symmetrische Perioden. Dabei ist es übrigens sehr wohl möglich, dass schon mit einem früheren Zeiger eine unsymmetrische Periode anhebt, wie in folgendem Beispiele für $K = \frac{\sqrt{19}+3}{2}$.

			1. symm. Periode						2. symm. Periode						
$n =$	−1	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$P_n =$		3	3	2	4	4	2	3	3	2	4	4	2	3	...
$Q_n =$	5	2	5	3	1	3	5	2	5	3	1	3	5	2	...
$a_n =$		3	1	2	8	2	1	3	1	2	8	2	1	3	...
		1. nicht symm. Periode						2. nicht symm. Periode							

Hier sind schon für den Zeiger 0 die Bedingungen (1), (2), (3) des §. 62 erfüllt, indem $2 < \sqrt{19} + 3$, $3 < \sqrt{19}$, $3 + 2 > \sqrt{19}$ ist. Demnach muss die Periode schon mit dem Zeiger 0 anheben, was sie auch wirklich thut. Diese Periode ist jedoch nicht symmetrisch.

Da für $m = 0$ die Grösse $\frac{2P_m}{Q_m} = \frac{2P_0}{Q_0} = \frac{2.3}{2} = 3$, also gleich einer ganzen Zahl ist; so muss vom Zeiger 1 an eine sym-

metrische Periode vorhanden sein, deren letzter Quotient $a_n = 2a_m - \frac{2P_m}{Q_m} = 2.3 - \frac{2.3}{2} = 3$ ist. Auch Dieses findet sich bestätigt.

III. Symmetrie der Periode für spezielle Fälle. Aus dem gegenwärtigen und dem vorhergehenden Paragraphen leuchtet ein, dass in allen Fällen, wo $P_0 = 0$ ist, eine symmetrische Periode vorhanden ist. Dieselbe beginnt für $\sqrt{D}$ und $\frac{\sqrt{D}}{Q_0} > 1$ mit dem Zeiger 1 und für $\frac{\sqrt{D}}{Q_0} < 1$ mit dem Zeiger 2.

Für diese drei Fälle nimmt die Periode am Anfange und am Ende folgende Gestalt an, wenn man $D = a^2 + b$, $\frac{D - P_0^2}{Q_0} = \frac{D}{Q_0} = Q_{-1}$ und für den Fall, dass $\frac{\sqrt{D}}{Q_0} > 1$ ist, die grössten in $\frac{\sqrt{D}}{Q_0}$ enthaltenen Ganzen $= g$ und für den Fall, dass $\frac{\sqrt{D}}{Q_0} < 1$ ist, die grössten in $\frac{Q_0}{\sqrt{D}}$ enthaltenen Ganzen $= h$ setzt.

für $K = \sqrt{D}$

$n =$	-1	0	1	$2 \dots$	$n-2$	$n-1$	n	$n+1$	$n+2 \dots$
$P_n =$		0	a	P_2		P_2	a	a	P_2
$Q_n =$	D	1	b	Q_2	Q_2	b	1	b	Q_2
$a_n =$		a	a_1	a_2	a_2	a_1	$2a$	a_1	a_2

für $K = \frac{\sqrt{D}}{Q_0} > 1$

$n =$	-1	0	1	$2 \dots$	$n-2$	$n-1$	n	$n+1$	$n+2 \dots$
$P_n =$		0	gQ_0	P_2		P_2	gQ_0	gQ_0	P_2
$Q_n =$	Q_{-1}	Q_0	Q_1	Q_2	Q_2	Q_1	Q_0	Q_1	Q_2
$a_n =$		g	a_1	a_2	a_2	a_1	$2g$	a_1	a_2

für $K = \frac{\sqrt{D}}{Q_0} < 1$

$n =$	-1	0	1	2	$3 \dots$	$n-2$	$n-1$	n	$n+1$	$n+2 \dots$
$P_n =$		0	0	hQ_{-1}	P_3		P_3	hQ_{-1}	hQ_{-1}	P_3
$Q_n =$	Q_{-1}	Q_0	Q_{-1}	Q_2	Q_3	Q_3	Q_2	Q_{-1}	Q_2	Q_3
$a_n =$		0	h	a_2	a_3	a_3	a_2	$2h$	a_2	a_3

So hat man z. B. nach §. 60 Beispiel 6 für $K = \sqrt{29}$

$n =$	-1	0	1	2	3	4	5	6	$7 \dots$
$P_n =$		0	5	3	2	3	5	5	$3 \dots$
$Q_n =$	29	1	4	5	5	4	1	4	$5 \dots$
$a_n =$		5	2	1	1	2	10	2	$1 \dots$

Endlich ist klar, dass wenn $Q_0 = 2$ ist, die Periode stets symmetrisch sein muss, indem dann $\frac{2P_0}{Q_0} = P_0$ ist. Alle Grössen $K = \frac{\sqrt{D} + P_0}{2}$ haben also symmetrische Perioden. Ebenso ist für $Q_0 = 1$ stets eine symmetrische Periode vorhanden.

§. 65. Maxima und Minima in der Periode.

I. Wenn irgend ein positives $Q_m \leqq a$ ist; so müssen alle Grössen P und Q, sowie alle Quotienten vom nächstfolgenden Zeiger $m+1$ an in der Gesammtperiode liegen, und da die Grössen Q sich immer schon von einem um 1 kleineren Zeiger, als die Grössen P und die Quotienten wiederholen; so muss eine Einzelperiode der Grössen Q auch schon mit dem Zeiger m beginnen.

Denn es erhellet aus §. 61, dass unter solchen Umständen, gleichviel ob P_m positiv oder negativ ist,

(1) P_{m+1} positiv und $\leqq a$, ferner dass

(2) $$Q_{m+1} \leqq a + P_{m+1}$$

und dass, weil $\sqrt{D} + P_{m+1} > Q_m$, also auch

$$(\sqrt{D} + P_{m+1})\,(\sqrt{D} - P_{m+1}) > Q_m\,(\sqrt{D} - P_{m+1})$$

$$\frac{D - P_{m+1}^2}{Q_m} > \sqrt{D} - P_{m+1} \text{ oder } Q_{m+1} > \sqrt{D} - P_{m+1} \text{ folglich}$$

(3) $$P_{m+1} + Q_{m+1} > \sqrt{D} \text{ oder } \geqq a + 1$$

ist, dass also für den Zeiger $m+1$ die in §. 62 für ein Glied der Periode aufgestellten drei Bedingungen erfüllt sind.

II. Hieraus erhellet, dass jedes positive Q, welches $\leqq a$ ist, nur in der Periode dieser Grössen liegen kann.

Dass es aber jederzeit in dieser Periode derartige Werthe für Q gibt, welche $\leqq a$ sind, folgt aus der Beziehung $Q_{n-1}\,Q_n = D - P_n^2$. Denn da in der Periode $P_n \leqq a$; so ist $D - P_n^2 = a^2 + b - P_n^2 \leqq a^2 + b$ also

$$Q_{n-1}\,Q_n < (a+1)^2$$

Hieraus erhellet, dass jedenfalls Einer der beiden Faktoren Q_{n-1}, Q_n (oder beide) $\leqq a$ sein muss.

Aus Vorstehendem folgt, dass das positive Minimum der Grössen Q in der Periode dieser Grössen liegt.

Auch ist aus der Beziehung $Q_{n-1}\,Q_n < (a+1)^2$ klar, dass in der Periode der Q auf ein Q, welches $\leqq a$ ist, sowol ein anderes Q folgen kann, welches ebenfalls $\leqq a$, als auch Eines, welches $> a$ ist, dass jedoch auf ein Q, welches $> a$ ist, nur ein anderes folgen kann, welches $\leqq a$ ist.

Die positiven, ausserhalb der Periode liegenden Q sind sämmtlich $> a$.

Was die etwa vorhandenen negativen Werthe von Q, welche nur ausserhalb der Periode liegen können, betrifft; so wird man aus späteren Untersuchungen (§. 71, II.) erkennen, dass diejenigen derselben, deren absolute Werthe $\leqq a$ sind, nur das Entgegengesetzte von solchen sein können, welche auch in der Periode liegen.

Demnach können andere absolute Werthe von $Q \leqq a$,

als welche in der Periode liegen, in der ganzen Entwickelung von K nirgends vorkommen.

Aus Vorstehendem erkennt man auch, dass wenn in dem gegebenen Ausdrucke $K = \frac{\sqrt{D} \pm P_0}{Q_0}$ die Grösse Q_0 positiv und $\leqq a$, ausserdem aber auch K positiv, also für den Fall, dass im Zähler das negative Zeichen gilt, $P_0 \leqq a$ ist, die Gesammtperiode mit dem Zeiger 1, die Einzelperiode der Q aber schon mit dem Zeiger 0 anfängt, und demnach negative Werthe von Q überall nicht vorkommen können.

Das Minimum von Q kann nicht kleiner als 1 sein. Der Werth 1 kann also, wenn er überhaupt unter jenen Grössen vorkommt, nur in der Periode erscheinen.

Das Maximum von Q in der Periode kann nicht den Werth $2a$ übersteigen. Wenn dieser Werth überhaupt unter den Grössen Q zum Vorschein kommt; so muss gleichzeitig $P = a$ und der Quotient $a_n = 1$ sein. (Im Übrigen kann der letztere Quotient auch noch unter andern Umständen $= 1$ werden.) Der höchstmögliche Werth $2a$ von Q stellt sich nach §. 64 stets bei der Entwickelung von $K = \sqrt{D}$ heraus, und zwar nur im letzten Gliede der Periode.

III. Das Minimum von P in der Periode kann nicht kleiner als 1 sein. Denn es ist schon in §. 62 unter den speziellen Fällen gezeigt, dass für ein positives Q der Werth $P = 0$ nicht einem Gliede der Periode angehören kann.

Das Maximum von P in der Periode kann den Werth a nicht übersteigen.

IV. Das Minimum der Quotienten a_n in der Periode kann nicht kleiner sein als 1.

Das Maximum dieser Quotienten in der Periode kann den Werth $2a$ nicht übersteigen, welcher sich einstellen würde, wenn $P = a$ und gleichzeitig $Q = 1$ wäre.

Sobald für den Zeiger n $Q = 1$ wird, muss nach §. 61 Gl. (22) oder (23), gleichviel ob P_n positiv oder negativ ist, $a_n = a + P_n$, $R_n = 0$, also $P_{n+1} = a$ und $Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n}$ $= \frac{a^2 + b - a^2}{1} = b$ werden.

§. 66. *Entwickelung der Grösse K in einen Kettenbruch in allgemeinen Zeichen für besondere Fälle.*

I. Wenn man berücksichtigt, wie die Zähler und Nenner der Näherungswerthe eines Kettenbruchs aus den Quotienten entstehen (namentlich nach dem independenten Gesetze des

§. 12) so kann der in §. 58 Gl. (5) und (6) nachgewiesene Zusammenhang zwischen den Grössen D, P_0, Q_0 und jenen Zählern und Nennern dazu dienen, um allgemeine Bedingungen aufzufinden, unter welchen die bei der Entwickelung von K entstehenden Grössen P_n, Q_n, a_n gewissen Anforderungen entsprechen. Insbesondere wird man auf diesem Wege Untersuchungen über die Merkmale der Grössen D, P_0, Q_0 anstellen können, welche erfüllt sein müssen, um Perioden von einer bestimmten Länge zu erhalten.

Derartige Betrachtungen würden jedoch hier zu weit führen; ich erlaube mir indessen die Bemerkung, dass die Behauptung von Lagrange in den Zusätzen zu Eulers Algebra, §. 36, wonach die Länge der Periode der von ihm betrachteten Grössen Q, P, welche sich von unseren Grössen P, Q nur durch das Zeichen unterscheiden, lediglich von der Determinante D, nicht aber von den Grössen P_0 und Q_0 abhängig sei, irrig ist. Dies lehren unter Anderem die Beispiele 3 und 5 in §. 60, indem $\frac{\sqrt{37}-4}{3}$ eine zweigliedrige, dagegen $\sqrt{37}$ eine eingliedrige Periode hat. Lagrange hat auch jene Behauptung ohne Beweis hingestellt. Es leuchtet übrigens ein, dass, um jene Behauptung zu bewahrheiten, nicht etwa je nach den Umständen von der kürzestmöglichen Periode der Grösse K irgend ein Vielfaches als Periode betrachtet werden darf, sondern dass es sich immer nur um die Periode von kleinster Länge handeln kann. Denn sonst könnte man behaupten, dass die Perioden aller möglichen Grössen K gleiche Länge hätten, indem man, wenn resp. für K und K' die kürzesten Perioden die Längen l und l' besässen, sowol für K, als auch für K' Perioden von der Länge ll' annähme.

II. Bemerkenswerth für die Entwickelung von $K=\sqrt{D}$ sind die Fälle, wo in der Determinante $D=a^2+b$ die Grösse b ein Faktor von $2a$ ist, wo man also $b=\frac{2a}{p}$ hat. Dies gibt sofort folgende Entwickelung für $K=\sqrt{a^2+b}=\sqrt{a^2+\frac{2a}{p}}$

$n=$	-1	0	1	2	3	4	...
$P_n=$		0	a	a	a	a	...
$Q_n=$	b	1	b	1	b	1	...
$a_n=$		a	p	$2a$	p	$2a$	...

$$(1)\qquad \sqrt{a^2+\frac{2a}{p}}=[a,\underbrace{p,\ 2a,}\underbrace{p,\ 2a,}\underbrace{p,\ 2a}\ldots]$$

Zwischen dem vollkommenen Quadrate von a und dem nächst höheren Quadrate, also zwischen a^2 und $(a+1)^2 = a^2 + 2a + 1$, in welchem Zwischenraume die Determinante $D = a^2 + b$ liegt, gibt es in allen Fällen wenigstens vier Zahlen, für welche die obige Bedingung $b = \frac{2a}{p}$ erfüllt ist, nämlich wenn

	$b = 1$	2	a	$2a$
also	$D = a^2+1$	a^2+2	a^2+a	a^2+2a
und	$p = 2a$	a	2	1

ist. Für die Form $D = a^2 + 1$ werden alle Grössen $P = a$, alle Grössen $Q = 1$ und alle Quotienten mit Ausnahme des ersten $= 2a$ und man hat

(2) $$\sqrt{a^2+1} = [a, 2a, 2a, 2a, 2a \ldots]$$

Ferner hat man für die andern drei Fälle

(3) $$\sqrt{a^2+2} = [a, a, 2a, a, 2a \ldots]$$

(4) $$\sqrt{a^2+a} = [a, 2, 2a, 2, 2a \ldots]$$

(5) $$\sqrt{a^2+2a} = [a, 1, 2a, 1, 2a \ldots]$$

So hat man z. B.

$$\sqrt{26} = \sqrt{5^2+1} = [5, 10, 10, 10, 10 \ldots]$$
$$\sqrt{27} = \sqrt{5^2+2} = [5, 5, 10, 5, 10 \ldots]$$
$$\sqrt{30} = \sqrt{5^2+5} = [5, 2, 10, 2, 10 \ldots]$$
$$\sqrt{35} = \sqrt{5^2+2.5} = [5, 1, 10, 1, 10 \ldots]$$
$$\sqrt{40} = \sqrt{6^2+4} = \sqrt{6^2 + \frac{2.6}{3}} = [6, 3, 12, 3, 12 \ldots]$$

III. Um das charakteristische Merkmal von K zu entdecken, welches zu einem Kettenbruche mit l a u t e r g l e i c h e n Q u o t i e n t e n c führt, sodass also $K = [c, c, c, c \ldots]$ wird, setzen wir in §. 58, Gl. (5) $n = 0$, $r = 1$; Dies gibt

$$(N_{-1}N_1 - N_0N_0)K^2 - (M_{-1}N_1 + M_1N_{-1} - M_0N_0 - M_0N_0)K + (M_{-1}M_1 - M_0M_0) = 0$$

oder da $M_{-1} = 1$, $N_{-1} = 0$, $M_0 = c$, $N_0 = 1$, $M_1 = c^2 + 1$, $N_1 = c$ ist,

$$-K^2 + cK + 1 = 0$$

Hieraus folgt

(6) $$K = \sqrt{\left(\frac{c}{2}\right)^2 + 1} + \frac{c}{2} = \frac{\sqrt{c^2+4}+c}{2} = [c, c, c, c \ldots]$$

Jenachdem c paar oder unpaar ist, hat man sich des ersten oder des zweiten Ausdrucks für K zu bedienen. Die Wurzelgrösse ist stets positiv, da $K > c$ ist.

So hat man z. B.

$$\sqrt{10} + 3 = \sqrt{\left(\frac{6}{2}\right)^2 + 1} + \frac{6}{2} = [6, 6, 6, 6 \ldots]$$

$$\frac{\sqrt{29}+5}{2} = \frac{\sqrt{5^2+4}+5}{2} = [5, 5, 5, 5 \ldots]$$

Subtrahirt man von K in Gl. (6) die vor dem Kettenbruche stehenden Ganzen c; so erhält man

$$(7)\quad \sqrt{\left(\frac{c}{2}\right)^2+1}-\frac{c}{2}=\frac{\sqrt{c^2+4}-c}{2}=[0,\ c,\ c,\ c\ldots]$$

$$\text{z. B. } \frac{\sqrt{5}-1}{2}=\frac{\sqrt{1^2+4}-1}{2}=[0,\ 1,\ 1,\ 1\ldots]$$

Addirt man zu dem letzteren Werthe die ganze Zahl d; so kommt

$$(8)\quad \sqrt{\left(\frac{c}{2}\right)^2+1}+d-\frac{c}{2}=\frac{\sqrt{c^2+4}+2d-c}{2}=[d,\ c,\ c,\ c\ldots]$$

In der Gl. (8) kann d auch eine negative Zahl sein, wogegen c stets positiv sein muss. So hat man z. B.

$$\sqrt{10}-11=\sqrt{\left(\frac{6}{2}\right)^2+1}-8-\frac{6}{2}=[-8,\ 6,\ 6,\ 6\ldots]$$

IV. Will man die Werthe von K untersuchen, welche Kettenbrüche mit einer schon bei dem Zeiger 0 anhebenden zweigliedrigen Periode c, d ergeben, sodass $K=[c,\ d,\ c,\ d\ldots]$ ist; so hat man in §. 58, Gl. (5) $n=1$, $r=2$ zu setzen. Dies gibt

$$(N_0N_3-N_1N_2)K^2-(M_0N_3+M_3N_0-M_1N_2-M_2N_1)K+(M_0M_3-M_1M_2)=0$$

und da $M_0=c$, $N_0=1$, $M_1=cd+1$, $N_1=d$, $M_2=c^2d+2c$, $N_2=cd+1$, $M_3=c^2d^2+3cd+1$, $N_3=cd^2+2d$ ist,

$$dK^2-cdK-c=0$$

Hieraus folgt

$$(9)\quad K=\sqrt{\left(\frac{c}{2}\right)^2+\frac{c}{d}}+\frac{c}{2}=\frac{\sqrt{cd(cd+4)}+cd}{2d}=[c,\ d,\ c,\ d\ldots]$$

In der ersten Form von K wird vorausgesetzt, dass sowol $\frac{c}{2}$, wie $\frac{c}{d}$ eine ganze Zahl sei, wie z. B. in

$$K=\sqrt{39}+6=\sqrt{\left(\frac{12}{2}\right)^2+\frac{12}{4}}+\frac{12}{2}=[12,\ 4,\ 12,\ 4\ldots]$$

Die zweite Form von K ist in allen hierher gehörigen Fällen brauchbar, z. B. für

$$K=\frac{\sqrt{285}+15}{6}=\frac{\sqrt{5.3\,(5.3+4)}+5.3}{2.3}=[5,\ 3,\ 5,\ 3\ldots]$$

Wenn $\frac{c}{d}$ oder auch schon $\frac{4c}{d}$, nicht aber $\frac{c}{2}$ eine ganze Zahl ist, hat man die Form

(10) $$K = \frac{\sqrt{c^2 + \frac{4c}{d}} + c}{2} = [c, d, c, d \ldots]$$

Wenn $\frac{c}{2}$ oder auch schon $\frac{cd}{2}$, nicht aber $\frac{c}{d}$ eine ganze Zahl ist, hat man die Form

(11) $$K = \frac{\sqrt{\left(\frac{cd}{2}\right)^2 + cd} + \frac{cd}{2}}{d} = [c, d, c, d \ldots]$$

Was die Grössen P, Q für die zweite Form in Gl. (9), also für $K = \frac{\sqrt{cd\,(cd+4)} + cd}{2d}$ betrifft; so ist die vollständige Entwickelung

$n =$	-1	0	1	2	$3 \ldots$
$P_n =$		cd	cd	cd	$cd \ldots$
$Q_n =$	$2c$	$2d$	$2c$	$2d$	$2c \ldots$
$a_n =$		c	d	c	$d \ldots$

Jenachdem für K die erste Form in Gl. (9) oder die Form in Gl. (10) oder die Form in Gl. (11) gilt, hat man die vorstehenden Werthe von P_n und Q_n resp. mit cd oder mit d oder mit 2 zu dividiren.

Subtrahirt man von irgend Einer dieser vier Formen von K den Werth der vor dem Kettenbruche stehenden Ganzen c; so erhält man die betreffende Form, welche den Kettenbruch $[0, d, c, d, c, \ldots]$ erzeugt. Dies gibt z. B. für die zweite Form in Gl. (9)

(12) $$\frac{\sqrt{cd\,(cd+4)} - cd}{2d} = [0, d, c, d, c \ldots]$$

Addirt man hierzu die ganze Zahl f; so ergibt sich

(13) $$\frac{\sqrt{cd\,(cd+4)} + d\,(2f-c)}{2d} = [f, d, c, d, c \ldots]$$

§. 67. ***Beziehungen zwischen zwei Einzelwerthen der Grössen P, Q und sämmtlichen in der Entwickelungsreihe vorhergehenden Grössen dieser Art.***

I. Aus den Werthen der Reihen (1), (2) in §. 61 ergibt sich

$$P_n = a_{n-1}\,Q_{n-1} - P_{n-1} = a_{n-1}\,Q_{n-1} - a_{n-2}\,Q_{n-2} + P_{n-2}$$
$$= a_{n-1}\,Q_{n-1} - a_{n-2}\,Q_{n-2} + a_{n-3}\,Q_{n-3} - P_{n-3}$$

u. s. w.; allgemein, wenn r eine unpaare Zahl ist,

(1) $$P_n + P_{n-r} = a_{n-1}\,Q_{n-1} - a_{n-2}\,Q_{n-2} + a_{n-3}\,Q_{n-3} - \ldots + a_{n-r}\,Q_{n-r}$$

und wenn r eine paare Zahl ist,

(2) $$P_n - P_{n-r} = a_{n-1}\,Q_{n-1} - a_{n-2}\,Q_{n-2} + a_{n-3}\,Q_{n-3} - \ldots - a_{n-r}\,Q_{n-r}$$

Demnach hat man, wenn n unpaar ist,

(3) $$P_0 + P_n = a_0\,Q_0 - a_1\,Q_1 + a_2\,Q_2 - \ldots - a_{n-2}\,Q_{n-2} + a_{n-1}\,Q_{n-1}$$

und wenn n paar ist,

(4) $P_0 - P_n = a_0 Q_0 - a_1 Q_1 + a_2 Q_2 - \ldots + a_{n-2} Q_{n-2} - a_{n-1} Q_{n-1}$

Ferner folgt aus den Werthen der Reihe (3), (4) in §. 61

$$Q_n = \frac{(D - P_n^2)}{Q_{n-1}} = \frac{(D - P_n^2) Q_{n-2}}{(D - P_{n-1}^2)} = \frac{(D - P_n^2)(D - P_{n-2}^2)}{(D - P_{n-1}^2) Q_{n-3}}$$

u. s. w.; allgemein, wenn r eine unpaare Zahl ist,

$$(5) \qquad Q_n Q_{n-r} = \frac{(D - P_n^2)(D - P_{n-2}^2) \ldots (D - P_{n-r+1}^2)}{(D - P_{n-1}^2)(D - P_{n-3}^2) \ldots (D - P_{n-r+2}^2)}$$

und wenn r eine paare Zahl ist

$$(6) \qquad \frac{Q_n}{Q_{n-r}} = \frac{(D - P_n^2)(D - P_{n-2}^2) \ldots (D - P_{n-r+2}^2)}{(D - P_{n-1}^2)(D - P_{n-3}^2) \ldots (D - P_{n-r+1}^2)}$$

Demnach hat man, wenn n unpaar ist,

$$(7) \qquad Q_0 Q_n = \frac{(D - P_1^2)(D - P_3^2) \ldots (D - P_n^2)}{(D - P_2^2)(D - P_4^2) \ldots (D - P_{n-1}^2)}$$

und wenn n paar ist,

$$(8) \qquad \frac{Q_n}{Q_0} = \frac{(D - P_2^2)(D - P_4^2) \ldots (D - P_n^2)}{(D - P_1^2)(D - P_3^2) \ldots (D - P_{n-1}^2)}$$

II. Es sei m irgend ein in der Periode liegender Zeiger und r die Gliederzahl der Periode, sodass alle Grössen von den Zeigern m, $m+r$, $m+2r \ldots$ resp. einander gleich sind.

Ist dann die Gliederzahl r der Periode paar; so ergeben die Gleichungen (2) und (6) für $n-r=m$ und $n=m+r$

(9) $0 = a_m Q_m - a_{m+1} Q_{m+1} + \ldots + a_{m+r-2} Q_{m+r-2} - a_{m+r-1} Q_{m+r-1}$

$$(10) \qquad 1 = \frac{(D - P_{m+2}^2)(D - P_{m+4}^2) \ldots (D - P_{m+r}^2)}{(D - P_{m+1}^2)(D - P_{m+3}^2) \ldots (D - P_{m+r-1}^2)}$$

Ist dagegen die Gliederzahl r der Periode unpaar; so ergeben die Gleichungen (1) und (5) für dieselbe Substitution

(11) $2P_m = a_m Q_m - a_{m+1} Q_{m+1} + \ldots - a_{m+r-2} Q_{m+r-2} + a_{m+r-1} Q_{m+r-1}$

$$(12) \qquad Q_m^2 = \frac{(D - P_{m+1}^2)(D - P_{m+3}^2) \ldots (D - P_{m+r}^2)}{(D - P_{m+2}^2)(D - P_{m+4}^2) \ldots (D - P_{m+r-1}^2)}$$

Rechnet man aber im letzteren Falle $2r$ Glieder zu der Periode; so hat man eine Periode von paarer Gliederzahl, also nach Gl. (9) und (10)

(13) $0 = a_m Q_m - a_{m+1} Q_{m+1} + \ldots + a_{m+2r-2} Q_{m+2r-2} - a_{m+2r-1} Q_{m+2r-1}$

$$(14) \qquad 1 = \frac{(D - P_{m+2}^2)(D - P_{m+4}^2) \ldots (D - P_{m+2r}^2)}{(D - P_{m+1}^2)(D - P_{m+3}^2) \ldots (D - P_{m+2r-1}^2)}$$

III. Aus diesen Formeln lassen sich verschiedene interessante Schlüsse ziehen. Unter Anderem:

Wenn die Periode nur $r=1$ Glied besitzt; so ist nach Gl. (11) die periodische Grösse $P_m = \frac{1}{2} a_m Q_m$; es muss also entweder a_m oder Q_m oder beide paar sein. Ferner ist dann nach Gl. (12) $Q_m^2 = D - P_{m+1}^2 = D - P_m^2$, also $D = P_m^2 + Q_m^2$. Bei eingliedrigen Perioden muss also die Determinante die Summe zweier Quadrate sein, deren Wurzeln resp. als P_m und Q_m

auftreten werden. Dies findet sich in dem Beispiele 5 in §. 60 für $D=37=6^2+1^2$ bestätigt.

Wenn die Periode nur $r=2$ Glieder besitzt; so ist nach Gl. (9) $a_m Q_m = a_{m+1} Q_{m+1}$ und nach Gl. (10) $D-P_{m+1}^2 = D-P_{m+2}^2$ also $P_{m+1}=P_{m+2}$; es müssen also dann alle in der Periode liegende Grössen P einander gleich sein, was sich in allen betreffenden Beispielen des §. 60 bestätigt.

IV. Man kann auch noch die folgenden Formeln merken, welche sich aus den Reihen (9), (10) des §. 61 ergeben. Zuvörderst hat man für einen paaren Werth von r

$$(15)\quad \begin{cases} Q_n - Q_{n-r} = a_{n-1}(P_{n-1}-P_n) + a_{n-3}(P_{n-3}-P_{n-2}) + \ldots \\ \qquad + a_{n-r+1}(P_{n-r+1}-P_{n-r+2}) \end{cases}$$

Ist also n paar; so folgt daraus

$$(16)\quad Q_n - Q_0 = a_1(P_1-P_2) + a_3(P_3-P_4) + \ldots + a_{n-1}(P_{n-1}-P_n)$$

und wenn n unpaar ist,

$$(17)\quad Q_n - Q_{-1} = a_0(P_0-P_1) + a_2(P_2-P_3) + \ldots + a_{n-1}(P_{n-1}-P_n)$$

Liegt der Zeiger m in der Periode von r Gliedern; so hat man nach Gl. (15), wenn die Gliederzahl r der Periode paar ist,

$$(18)\quad \begin{cases} 0 = a_{m+1}(P_{m+1}-P_{m+2}) + a_{m+3}(P_{m+3}-P_{m+4}) + \ldots \\ \qquad + a_{m+r-1}(P_{m+r-1}-P_{m+r}) \end{cases}$$

Wenn aber die Gliederzahl r der Periode unpaar ist; so ergibt die Gleichung (15), indem man darin erst $r+1$ für r an die Stelle setzt und beachtet, dass $Q_{m-r-1}=Q_{m-1}$ ist,

$$(19)\quad \begin{cases} Q_m - Q_{m-1} = a_m(P_m-P_{m+1}) + a_{m+2}(P_{m+2}-P_{m+3}) + \ldots \\ \qquad + a_{m+r-1}(P_{m+r-1}-P_{m+r}) \end{cases}$$

§. 68. *Beziehungen zwischen den Grössen P, Q und den Zählern und Nennern M, N der Näherungsbrüche.*

I. Von Wichtigkeit ist die Bestimmung der Grössen P, Q mittelst der Zähler und Nenner der vorhergehenden Näherungswerthe von K.

Da $M_{-2}=0$, $N_{-2}=1$, $M_{-1}=1$, $N_{-1}=0$ ist; so kann man zuvörderst schreiben

$$-Q_{-1} = M_{-2}^2 Q_0 - 2M_{-2}N_{-2}P_0 - N_{-2}^2 Q_{-1}$$
$$-P_0 = M_{-1}M_{-2}Q_0 - (M_{-1}N_{-2}+M_{-2}N_{-1})P_0 - N_{-1}N_{-2}Q_{-1}$$
$$Q_0 = M_{-1}^2 Q_0 - 2M_{-1}N_{-1}P_0 - N_{-1}^2 Q_{-1}$$

Ferner hat man, da $M_0=a_0$, $N_0=1$ ist, nach den obersten Formeln der Reihen (1), (2) und (5), (6) in §. 61 sofort

$$P_1 = M_0 M_{-1} Q_0 - (M_0 N_{-1} + M_{-1} N_0) P_0 - N_0 N_{-1} Q_{-1}$$
$$-Q_1 = M_0^2 Q_0 - 2M_0 N_0 P_0 - N_0^2 Q_{-1}$$

Substituirt man diese Werthe von P_1 und Q_1 in die zweiten Formeln der eben genannten Reihen in §. 61; so kommt

$$-P_2 = M_1 M_0 Q_0 - (M_1 N_0 + M_0 N_1) P_0 - N_1 N_0 Q_{-1}$$
$$Q_2 = M_1^2 Q_0 - 2M_1 N_1 P_0 - N_1^2 Q_{-1}$$

Eine Substitution dieser Werthe von P_2 und Q_2 in die dritten Formeln der genannten Reihen gibt

$$P_3 = M_2 M_1 Q_0 - (M_2 N_1 + M_1 N_2) P_0 - N_2 N_1 Q_{-1}$$
$$-Q_3 = M_2^2 Q_0 - 2 M_2 N_2 P_0 - N_2^2 Q_{-1}$$

Eine Fortsetzung dieses Verfahrens führt unter Beachtung der allgemeinen Formeln (1) und (5) in §. 61 zu dem leicht zu erweisenden sehr wichtigen Gesetze:

(1) $(-1)^{n-1} P_n = M_{n-1} M_{n-2} Q_0 - (M_{n-1} N_{n-2} + M_{n-2} N_{n-1}) P_0 - N_{n-1} N_{n-2} Q_{-1}$

(2) $(-1)^n Q_n = M_{n-1}^2 Q_0 - 2 M_{n-1} N_{n-1} P_0 - N_{n-1}^2 Q_{-1}$

II. Setzt man in diesen Gleichungen $Q_{-1} = \frac{D - P_0^2}{Q_0}$ und multiplizirt eine jede mit Q_0; so nehmen dieselben die gleichfalls sehr beachtenswerthe Gestalt

(3) $(-1)^{n-1} Q_0 P_n = (M_{n-1} Q_0 - N_{n-1} P_0)(M_{n-2} Q_0 - N_{n-2} P_0) - N_{n-1} N_{n-2} D$

(4) $(-1)^n Q_0 Q_n = (M_{n-1} Q_0 - N_{n-1} P_0)^2 - N_{n-1}^2 D$

an. Eliminirt man zwischen den letzteren Gleichungen (3) und (4) die Grösse D; so stellt sich die Beziehung

(5) $N_{n-2} Q_n + N_{n-1} P_n = M_{n-1} Q_0 - N_{n-1} P_0$

heraus.

III. Die Gl. (4) ergibt einen interessanten Ausdruck für den Näherungswerth $K_{n-1} = \frac{M_{n-1}}{N_{n-1}}$, wenn man mit N_{n-1}^2 dividirt und die entstehende Gleichung für K_{n-1} auflös't. Erhöhet man schliesslich die Zeiger n und $n-1$ um 1; so kommt

$$(6) \qquad K_n = \frac{M_n}{N_n} = \frac{\sqrt{D + (-1)^{n+1} \frac{Q_0 Q_{n+1}}{N_n^2}} + P_0}{Q_0}$$

Je grösser man n nimmt, desto grösser wird N_n und wächst mit n ins Unendliche, während die Grösse Q_{n+1} stets endlich bleibt. Man erkennt also aus dieser Formel, in welcher Weise sich mit wachsendem n der Näherungswerth K_n dem Gesammtwerthe K des ganzen Kettenbruchs nähert, und dass für $n = \infty$ genau $K_n = \frac{\sqrt{D} + P_0}{Q_0} = K$ wird. Diese Bemerkung ist von wesentlicher Bedeutung, indem dieselbe als Ergänzung zu dem Schlusssatze des §. 59 den Beweis liefert, dass eine Reduktion des aus der Entwickelung jenes Paragraphen hervorgehenden Kettenbruchs die Grösse $\frac{\sqrt{D} + P_0}{Q_0}$ nach Werth und Form genau wiedererzeugen müsse.

Ebenso wichtig ist der Werth, welcher sich für die Determinante D aus Gl. (4) ergibt. Derselbe ist, wenn man die Zeiger n und $n-1$ um 1 erhöhet,

$$(7) \qquad D = \frac{(M_n Q_0 - N_n P_0)^2 - (-1)^{n+1} Q_0 Q_{n+1}}{N_n^2}$$

Diese Formel führt zu einer sehr bequemen Reductionsformel für einen Kettenbruch, welcher die Quadratwurzel aus einer ganzen Zahl D darstellt, für welchen also $P_0 = 0$, $Q_0 = 1$ ist. Weiss man also bestimmt, dass man es mit einem solchen Kettenbruche, für welchen nur die Quotienten gegeben sein mögen, zu thun hat; so sei $n+1$ der letzte Zeiger der Periode, für welchen der Quotient $a_{n+1} = 2a$ ist. Alsdann weiss man aus §. 64, obgleich die Grössen Q gar nicht bekannt zu sein brauchen, dass $Q_{n+1} = Q_0 = 1$ sein muss. Hiernach erhält man aus Gl. (7), worin nun n den vorletzten Zeiger in der Periode bezeichnet,

$$(8) \qquad K = \sqrt{D} = \sqrt{\frac{M_n^2 + (-1)^n}{N_n^2}}$$

Nach dieser Formel würde man in dem schon in §. 58 behandelten Beispiele $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4 \ldots]$, wenn man schon voraus wüsste, dass K die Form $\sqrt{D}$ hätte, sofort

$$K = \sqrt{\frac{M_3^2 + (-1)^3}{N_3^2}} = \sqrt{\frac{8^2 - 1}{3^2}} = \sqrt{7} \text{ haben.}$$

Die Gleichung (8) zur Bestimmung von K gilt auch dann noch, wenn K die Form $\frac{\sqrt{D}}{Q_0}$ hat, aber > 1 ist. Denn man hat in §. 64 gesehen, dass für diesen Fall der Werth von Q_0 sich im letzten Gliede der Periode wiederholt. Ist also $n+1$ der letzte Zeiger der Periode, folglich n der vorletzte; so hat man $Q_{n+1} = Q_0$. Da nun auch hier $P_0 = 0$ ist; so folgt aus Gl. (7)

$$(9) \qquad K = \frac{\sqrt{D}}{Q_0} = \sqrt{\frac{M_n^2 + (-1)^n}{N_n^2}}$$

So hat man für das in §. 58 behandelte Beispiel $\frac{\sqrt{195}}{5}$ $= [2, \underbrace{1, 3, 1, 4,} \underbrace{1, 3, 1, 4} \ldots]$

$$K = \frac{\sqrt{D}}{Q_0} = \sqrt{\frac{M_3^2 + (-1)^3}{N_3^2}} = \sqrt{\frac{14^2 - 1}{5^2}} = \sqrt{\frac{39}{5}} = \frac{\sqrt{195}}{5}$$

Wäre $K = \frac{\sqrt{D}}{Q_0} < 1$; so ist die Formel (9) durchaus nicht zu gebrauchen. Man weiss jedoch aus §. 64, dass sich dann im letzten Gliede der Periode die Grösse $Q_{-1} = \frac{D - P_0^2}{Q_0} = \frac{D}{Q_0}$ wiederholt. Ist also auch hier $n+1$ der letzte Zeiger der Periode und n der vorletzte; so hat man $Q_{n+1} = Q_{-1} = \frac{D}{Q_0}$

Substituirt man diesen Werth für Q_{n+1} in Gl. (7), setzt $P_0 = 0$ und lös't die Gleichung für $\frac{D}{Q_0^2}$ auf; so kommt

$$(10) \qquad K = \frac{\sqrt{D}}{Q_0} = \sqrt{\frac{M_n^2}{N_n^2 - (-1)^n}}$$

So hat man z. B. für $\frac{\sqrt{195}}{39} = [0, 2, \underbrace{1, 3, 1, 4,}\underbrace{1, 3, 1, 4}\ldots]$

$$K = \frac{\sqrt{D}}{Q_0} = \sqrt{\frac{M_4^2}{N_4^2 - (-1)^4}} = \sqrt{\frac{5^2}{14^2 - 1}} = \sqrt{\frac{5}{39}} = \frac{\sqrt{195}}{39}$$

IV. Es wird noch darauf aufmerksam gemacht, dass wenn in den Gleichungen (1) bis (4) der Zeiger n in der Periode liegt, und die Periode eine paare Anzahl Glieder besitzt, die Grössen $(-1)^{n-1} P_n$ und $(-1)^n Q_n$ in Abständen von Einer Periodenlänge nicht bloss mit ihrem absoluten Werthe P_n, Q_n, sondern auch mit demselben Zeichen $(-1)^{n-1}$, $(-1)^n$ regelmässig wiederkehren, dass jedoch, wenn die Periode eine unpaare Anzahl Glieder enthält, jene Grössen in dem bezeichneten Abstande regelmässig das Zeichen wechseln, also immer in Abständen von zwei Periodenlängen mit demselben Zeichen wiederkehren.

V. Endlich theilen wir noch folgende interessante Formeln mit.

$$(11) \qquad \begin{cases} (-1)^n P_0 = M_{n-2} N_{n-2} Q_n + (M_{n-2} N_{n-1} + M_{n-1} N_{n-2}) P_n \\ \qquad - M_{n-1} N_{n-1} Q_{n-1} \end{cases}$$

$$(12) \qquad (-1)^n Q_0 = N_{n-2}^2 Q_n + 2 N_{n-2} N_{n-1} P_n - N_{n-1}^2 Q_{n-1}$$

$$(13) \qquad (-1)^{n-1} Q_{-1} = M_{n-2}^2 Q_n + 2 M_{n-2} M_{n-1} P_n - M_{n-1}^2 Q_{n-1}$$

Die Richtigkeit dieser Formeln erkennt man sofort, wenn man darin für P_n, Q_n, Q_{n-1} die nach den Formeln (1) und (2) gebildeten Ausdrücke substituirt.

Setzt man in diesen Gleichungen $Q_{n-1} = \frac{D - P_n^2}{Q_n}$; so nehmen dieselben folgende Form an.

$$(14) \qquad \begin{cases} (-1)^n P_0 Q_n = (M_{n-2} Q_n + M_{n-1} P_n)(N_{n-2} Q_n + N_{n-1} P_n) \\ \qquad - M_{n-1} N_{n-1} D \end{cases}$$

$$(15) \qquad (-1)^n Q_0 Q_n = (N_{n-2} Q_n + N_{n-1} P_n)^2 - N_{n-1}^2 D$$

$$(16) \qquad (-1)^{n-1} Q_{-1} Q_n = (M_{n-2} Q_n + M_{n-1} P_n)^2 - M_{n-1}^2 D$$

Eine Elimination der Grösse D zwischen den beiden Gleichungen (14) und (15) erzeugt die schon oben gefundene Formel (5). Eine Elimination zwischen (14) und (16) ergibt dagegen

$$(17) \qquad M_{n-2} Q_n + M_{n-1} P_n = N_{n-1} Q_{-1} + M_{n-1} P_0$$

§. 69. ***Entwickelung der Grösse K in einen Kettenbruch nach dem Additionsprinzipe mit Quotienten, welche den rationalen Theil der Grössen $x_0, x_1, x_2 \ldots$ am vollständigsten erschöpfen.***

I. Bisher haben wir nur eine Entwickelung der Grösse $K = \frac{\sqrt{D}+P_0}{Q_0}$ in einen Kettenbruch mit grössten Subquotienten betrachtet. Hiernach stellte der Quotient a_n, welcher aus der Formel

$$x_n = \frac{\sqrt{D}+P_n}{Q_n} = a_n + \frac{1}{x_{n+1}}$$

hervorging, den grössten Subquotienten von $\frac{\sqrt{D}+P_n}{Q_n}$ dar.

Es hat ein besonderes Interesse, auch diejenige Entwickelung von K zu betrachten, worin der Quotient a_n stets aus dem rationalen Theile von x_n, also aus dem Bruche $\frac{P_n}{Q_n}$ bestimmt wird, indem man für a_n immer diejenige positive oder negative ganze Zahl nimmt, welche diesem Bruche $\frac{P_n}{Q_n}$ am nächsten kommt, gleichviel ob sie grösser oder kleiner als jener Bruch wird. a_n ist also immer entweder der grösste Subquotient oder der kleinste Superquotient von $\frac{P_n}{Q_n}$, jenachdem der erste oder der zweite diesen Bruch am vollständigsten erschöpft. Läge der Werth von $\frac{P_n}{Q_n}$ genau in der Mitte zwischen diesen beiden Zahlen; so ist es gleichgültig, welche von beiden man für a_n annimmt: ein solcher Fall kann jedoch nur eintreten, wenn der Nenner des auf seine kleinste Benennung gebrachten Bruches $\frac{P_n}{Q_n}$ gleich 2 und der Zähler eine unpaare Zahl ist. Wenn Q_n in P_n aufgeht, hat man natürlich genau $a_n = \frac{P_n}{Q_n}$ zu nehmen.

Beispiel. $K = \frac{\sqrt{37}+2}{11}$, also $Q_{-1} = \frac{37-2^2}{11} = 3$.

Hier erhält man

$$x_0 = \frac{\sqrt{37}+2}{11} = 0$$
$$x_1 = \frac{\sqrt{37}-2}{3} = -1$$
$$x_2 = \frac{\sqrt{37}-1}{12} = 0$$
$$x_3 = \frac{\sqrt{37}+1}{3} = 0$$
$$x_4 = \frac{\sqrt{37}-1}{12} = x_2$$

n	P_n	Q_n	a_n
-1		3	
0	2	11	0
1	-2	3	-1
(2	-1	12	0
(3	1	3	0
(4	-1	12	0
(5	1	3	0

II. Die wichtigsten Eigenschaften der bei dieser Entwickelung auftretenden Grössen ergeben sich folgendermaassen. Es leuchtet ein, dass für diese Grössen die Beziehungen §. 61, Gl. (1) bis (14), sowie §. 67, Gl. (1) bis (14) und §. 68, Gl. (1) bis (7), sowie (11) bis (17) vollkommene Gültigkeit behalten. Setzt man also

(1) $$\frac{P_n}{Q_n} = a_n + \frac{R_n}{Q_n} \text{ also } P_n = a_n Q_n + R_n$$

so ist nach der Voraussetzung der numerische Werth des Restes R_n (welcher Rest selbst positiv oder negativ werden kann) durchaus $\leqq \frac{1}{2} Q_n$.

Für die nächstfolgende Grösse P vom Zeiger $n+1$ hat man nach der Grundformel §. 61 Gl. (2)

(2) $$P_{n+1} = a_n Q_n - P_n$$

d. i. nach Gl. (1)

(3) $$P_{n+1} = -R_n$$

Da nun numerisch genommen $R_n \leqq \frac{1}{2} Q_n$ ist; so erkennt man, dass auch

(4) $$P_{n+1} \leqq \frac{1}{2} Q_n$$

sei.

Es wird behauptet, dass man im Laufe der obigen Entwickelung auf einen Zeiger m stossen werde, für welchen nicht bloss laut der oben nachgewiesenen Beziehung $P_{m+1} \leqq \frac{1}{2} Q_m$, sondern für welchen auch gleichzeitig $P_{m+1} \leqq \frac{1}{2} Q_{m+1}$ ist, wobei die Grössen P, Q stets nach ihrem numerischen Werthe betrachtet werden.

Denn angenommen, dieser Zustand sei bei dem obigen Zeiger n noch nicht erreicht, es sei also

(5) $$P_{n+1} \leqq \frac{1}{2} Q_n, \text{ dagegen } P_{n+1} > \frac{1}{2} Q_{n+1}$$

so wird man für den nächstfolgenden Zeiger wegen der Beziehung (†)

(6) $$P_{n+2} \leqq \frac{1}{2} Q_{n+1}, \text{ also } P_{n+2} < P_{n+1}$$

haben.

Wäre der fragliche Zustand auch bei diesem Zeiger noch nicht erreicht, also

(7) $$P_{n+2} \leqq \frac{1}{2} Q_{n+1}, \text{ dagegen } P_{n+2} > \frac{1}{2} Q_{n+2}$$

so ergibt sich für den folgenden Zeiger

(8) $$P_{n+3} \leqq \frac{1}{2} Q_{n+2}, \text{ also } P_{n+3} < P_{n+2}$$

Hiernach werden die Grössen P_{n+1}, P_{n+2}, P_{n+3} ... numerisch immer kleiner, bis der fragliche Zustand eintritt, welcher nothwendig einmal eintreten muss, da man schliesslich auf einen Werth $P = 0$ kommen würde, für welchen jener Zustand offenbar vorhanden ist.

Endlich also hat man, numerisch genommen,

(9) $$P_{n+1} \leqq \frac{1}{2} Q_n \text{ und auch } \leqq \frac{1}{2} Q_{n+1}$$

oder was Dasselbe ist

(10) $$2P_{n+1} \leqq Q_n \text{ und auch } \leqq Q_{n+1}$$

III. Nachdem dieser Zustand erreicht ist, ist für den Zeiger $n+1$ und für jeden höheren der numerische Werth des Bruches $\frac{P_{n+1}}{Q_{n+1}} \leqq \frac{1}{2}$, also $a_{n+1} = 0$, folglich nach Gl. (2)

(11) $$-P_{n+1} = P_{n+2} = -P_{n+3} = P_{n+4} = \text{etc.}$$

sodass also von jener Stelle an die Grössen P einerlei numerischen Werth behalten, aber fortwährend das Zeichen wechseln.

IV. Ferner ist von der bezeichneten Stelle an

$$Q_{n+1} = Q_{n+1}$$
$$Q_{n+2} = \frac{D - P_{n+2}^2}{Q_{n+1}} = \frac{D - P_{n+1}^2}{Q_{n+1}} = Q_n$$
$$Q_{n+3} = \frac{D - P_{n+3}^2}{Q_{n+2}} = \frac{D - P_{n+1}^2}{Q_n} = Q_{n+1}$$
$$Q_{n+4} = \frac{D - P_{n+4}^2}{Q_{n+3}} = \frac{D - P_{n+1}^2}{Q_{n+1}} = Q_n$$

u. s. w., also

(12) $$Q_{n+1} = Q_{n+3} = Q_{n+5} = \text{etc.}$$

(13) $$Q_n = Q_{n+2} = Q_{n+4} = \text{etc.}$$

sodass also die um zwei Zeiger voneinander abstehenden Grössen Q fortwährend gleiche Werthe behalten.

V. Aus Vorstehendem folgt, dass die obige Entwickelung von K zu einer zweigliederigen Periode führen wird, welche von der Stelle an, wo man

$$P_{n+1} \leqq \tfrac{1}{2} Q_n \text{ und auch } < \tfrac{1}{2} Q_{n+1}$$

hat, folgendermaassen darzustellen ist.

$m =$	n	$n+1$	$n+2$	$n+3$	$n+4 \ldots$
$P_m =$		P_{n+1}	$-P_{n+1}$	P_{n+1}	$-P_{n+1} \ldots$
$Q_m =$	Q_n	Q_{n+1}	Q_n	Q_{n+1}	$Q_n \ldots$
$a_m =$		0	0	0	0 $\ldots$

VI. Da allgemein $Q_n Q_{n+1} = D - P_{n+1}^2$ ist; so folgt, dass für diese periodischen Werthe, wofür numerisch genommen $Q_n \geqq 2P_{n+1}$ und auch $Q_{n+1} > 2P_{n+1}$ ist, der numerische Werth der Differenz

$$D - P_{n+1}^2 \geqq 4P_{n+1}^2$$

ist. Damit Dies möglich sei, muss, weil D positiv ist, offenbar der numerische Werth von $P_{n+1} < D$ sein, da $P_{n+1}^2 - D$ unmöglich $\geqq 4P_{n+1}^2$ sein könnte. Man hat also

(14) $$D \geqq 5P_{n+1}^2 \text{ oder } P_{n+1} \leqq \sqrt{\frac{D}{5}}.$$

Ferner folgt aus der Beziehung $Q_n Q_{n+1} = D - P_{n+1}^2$, weil numerisch $P_{n+1} < D$ ist, dass die beiden periodischen Grössen Q_n und Q_{n+1} gleiche Zeichen haben und dass Eine von beiden numerisch $< \sqrt{D}$ ist.

§. 70. Entwickelung der Grösse K in einen Kettenbruch nach dem Additionsprinzipe mit willkürlichen Quotienten.

I. Ähnlich wie in §. 18 bei der Entwickelung eines rationalen Bruches, so kann man auch bei der Entwickelung der irrationalen Grösse $K = \frac{\sqrt{D}+P_0}{Q_0}$ willkürliche Quotienten in die Rechnung stellen. Die Grössen P und Q sind stets nach den bekannten Regeln des §. 59 zu bilden. So sind z. B. in der nachstehenden Entwickelung von $K = \frac{\sqrt{10}+2}{3}$, worin $D = 10 = 3^2+1$, $a = 3$, $Q_{-1} = \frac{10-2^2}{3} = 2$ ist. Die Quotienten $a_0, a_1, a_2, a_3, a_4, a_5 = 3, 1, -2, 1, 0, 2$ ganz willkürlich angenommen.

$$x_0 = \frac{\sqrt{10}+2}{3} = 3 + \frac{1}{x_1}$$

$$x_1 = \frac{3}{\sqrt{10}-7} = \frac{\sqrt{10}+7}{-13} = 1 + \frac{1}{x_2}$$

$$x_2 = \frac{-13}{\sqrt{10}+20} = \frac{\sqrt{10}-20}{30} = -2 + \frac{1}{x_3}$$

$$x_3 = \frac{30}{\sqrt{10}+40} = \frac{\sqrt{10}-40}{-53} = 1 + \frac{1}{x_4}$$

$$x_4 = \frac{-53}{\sqrt{10}+13} = \frac{\sqrt{10}-13}{3} = 0 + \frac{1}{x_5}$$

$$x_5 = \frac{3}{\sqrt{10}-13} = \frac{\sqrt{10}+13}{-53} = 2 + \frac{1}{x_6}$$

$$x_6 = \frac{-53}{\sqrt{10}+119} = \frac{\sqrt{10}-119}{267} = \text{etc.}$$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		2		1	0
0	2	3	3	3	1
1	7	-13	1	4	1
2	-20	30	-2	-5	-1
3	-40	-53	1	-1	0
4	-13	3	0	-5	-1
5	13	-53	2	-11	-2
6	-119	267			

Zwischen den in einer solchen Entwickelung auftretenden Grössen P_n, Q_n, a_n bestehen offenbar die Beziehungen §. 61, Gl. (1) bis (14), ferner §. 67 Gl. (1) bis (14) und §. 68 Gl. (1) bis (7), sowie (11) bis (17).

II. Ungültig werden jedoch im Allgemeinen alle übrigen bisher erläuterten Gesetze, namentlich die über die Periodizität, sowie die darauf sich stützenden Reduktionsformeln in §. 58 und die Sätze über Maxima und Minima in §. 65. Man könnte ja hier, wenn man wollte, ins Unendliche fortfahren, für die willkürlichen Quotienten eine jede beliebige Periode einzuführen.

Ein solcher periodischer Kettenbruch könnte zwar nach §. 58 wieder auf die Form $K' = \frac{\sqrt{D'} + P'_0}{Q'_0}$ reduzirt werden; allein der sich ergebende Werth von K' würde mit dem von K nicht übereinstimmen. Denn einestheils würde auf die gewärtige willkürliche Entwickelung die Schlussbemerkung in §. 59 über die abnehmende Fehlergränze keine Anwendung finden, anderentheils würde die Gl. (6) in §. 68 keine Übereinstimmung zwischen K' und K bei unendlich wachsendem n erweisen, weil bei der vorstehenden Willkürlichkeit die Grössen Q_n nicht periodisch werden, vielmehr im Allgemeinen ins Unendliche wachsen, sodass für einen unendlich grossen Zeiger n, selbst wenn dafür $N_n = \infty$ würde, doch $\frac{Q_0 Q_{n+1}}{N_n^2}$ nicht $= 0$ werden würde.

III. Um übrigens eine konvergente und auf den ursprünglichen Werth von K genau reduzirbare Kettenbruchsentwickelung zu erhalten, ist es nicht durchaus nothwendig, dass man fortwährend nach dem früheren Prinzipe der grössten Subquotienten verfahre. Man könnte auch nach dem Prinzipe der kleinsten Superquotienten verfahren. In diesem Falle würden alle Quotienten des Kettenbruchs, mit eventueller Ausnahme des ersten a_0, negativ werden, wie in folgendem Beispiele

$$K = \frac{\sqrt{11} + 9}{7},\ D = 11 = 3^2 + 2,\ a = 3,\ Q_{-1} = \frac{11 - 9^2}{7} = -10.$$

$$x_0 = \frac{\sqrt{11} + 9}{7} = 2 + \frac{1}{x_1}$$

$$x_1 = \frac{7}{\sqrt{11} - 5} = \frac{\sqrt{11} + 5}{-2} = -4 + \frac{1}{x_2}$$

$$x_2 = \frac{-2}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{-1} = -6 + \frac{1}{x_3}$$

$$x_3 = \frac{-1}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{-2} = -3 + \frac{1}{x_4}$$

$$x_4 = \frac{-2}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{-1} = x_2$$

n	P_n	Q_n	a_n
-1		-10	
0	9	7	2
1	5	-2	-4
2	3	-1	-6
3	3	-2	-3
4	3	-1	-6
5	3	-2	-3

$$K = \frac{\sqrt{11}+9}{7} = [2, -4, \underbrace{-6, -3}, \underbrace{-6, -3}\ldots]$$

Auch kann man mit gleichem Erfolge nach einer bestimmten Reihenfolge grösste Sub- mit kleinsten Superquotienten abwechseln lassen. Unter den Quotienten werden alsdann von einer gewissen Stelle an in einem regelmässigen Turnus positive mit negativen Zahlen abwechseln.

IV. Wir übergehen hier die nähere Erörterung der Gesetze, welche unter solchen Umständen an den Grössen P, Q, M, N sich bekunden werden, stellen aber über den Einfluss einer anfänglich willkürlichen Entwickelung noch folgende wesentliche Betrachtungen an.

Nachdem man die Grösse $K = \frac{\sqrt{D}+P_0}{Q_0}$ mit ganz beliebigen Quotienten bis zu irgend einem Zeiger $n-1$ entwickelt hat, sodass $a_0, a_1 \ldots a_{n-1}$ ganz willkürliche Werthe haben, kann man offenbar die Entwickelung der Grösse

$$x_n = \frac{\sqrt{D}+P_n}{Q_n} = a_n + \frac{1}{x_{n+1}}$$

genau nach dem Prinzipe der grössten Subquotienten fortsetzen. Dies muss, da x_n ganz und gar eine Grösse von der Beschaffenheit wie K ist, zur Folge haben, dass die folgenden Quotienten $a_n, a_{n+1} \ldots$, mit Ausnahme des ersten a_n, welcher nach den Umständen positiv, negativ oder null werden kann, sämmtlich positiv und von einer gewissen Stelle an periodisch werden, sowie auch, dass die Grössen P, Q von derselben Stelle an positiv und periodisch werden und den einer solchen Periode zukommenden Bedingungen entsprechen.

Es wird nun die sehr wichtige Behauptung ausgesprochen, dass die auf diese Weise entstehende Gesammtperiode der Grössen P, Q und der Quotienten genau dieselbe ist, welche sich herausstellen würde, wenn man gleich von vorn herein die Grösse K nur mit grössten Subquotienten entwickelt hätte, auch dass von einer gewissen Stelle an die Näherungswerthe beider Entwickelungen identisch werden.

V. Zum Beweise dieses Satzes zeigen wir zuerst, dass von einer gewissen Stelle die Quotienten und die Näherungswerthe von K und K' übereinstimmen.

Es ist nach §. 57 klar, dass unterhalb des Zeigers, bei welchem man angefangen hat, die willkürlich begonnene Entwickelung von K' nach dem Prinzipe der grössten Subquotienten fortzuführen, endlich eine Stelle erreicht werden wird, von wo an alle späteren Näherungswerthe $K'_m, K'_{m+1}, K'_{m+2} \ldots$ dem Werthe $K' = K$ sich wirklich unausgesetzt nähern und von

den absoluten Werthen der Zähler M'_m, M'_{m+1}, M'_{m+2}... und der Nenner N'_m, N'_{m+1}, N'_{m+2}... jener Näherungsbrüche jeder spätere grösser ist, als der vorhergehende, während die Quotienten a'_m, a'_{m+1}, a'_{m+2}... sämmtlich positiv $\geqq 1$ sind. Liessen sich nun diese Näherungswerthe von K' als der untere Theil einer ununterbrochenen Reihe von Näherungswerthen eines Kettenbruchs darstellen, welcher vom zweiten Quotienten an nur positive Quotienten $\geqq 1$ enthielte; so müsste offenbar dieser Kettenbruch mit der Entwickelung der Grösse $K'=K$ nach dem Prinzipe der grössten Subquotienten ganz identisch sein.

Um Dies zu zeigen, entwickeln wir den gemeinen rationalen Bruch K'_m, dessen Zähler und Nenner M'_m, N'_m sind, und welcher den reduzirten Werth des oberen Theiles a'_0, a'_1... a'_m der zum Theil willkürlichen Quotienten der Entwickelung K' darstellt, in einen Kettenbruch mit grössten Subquotienten. Dies gebe den Werth K_n, dessen Zähler und Nenner M_n, N_n und dessen Quotienten a_0, a_1... a_n seien, welche Letzteren vom zweiten a_1 an durchaus positiv sein werden. Jetzt hat man für die Zähler und Nenner der letzten Näherungswerthe von K_n und K'_m die Gleichheit $M_n=M'_m$ und $N_n=N'_m$. Was die vorletzten Zähler und Nenner betrifft; so brauchen dieselben zwar nicht einander gleich zu sein; es besteht aber zwischen denselben folgende Beziehung. Da

$$M'_{m-1}N'_m - M'_m N'_{m-1} = \pm (M_{n-1}N_n - M_n N_{n-1})$$

ist, indem der absolute Werth einer jeden Seite $=1$ ist (§. 4); so hat man, wenn man M'_m, N'_m mit M_n, N_n vertauscht,

$$(M'_{m-1} \mp M_{n-1})N_n = (N'_{m-1} \mp N_{n-1})M_n$$

und da M_n und N_n relativ prim sind; so muss

$$\frac{M'_{m-1} \mp M_{n-1}}{M_n} = \frac{N'_{m-1} \mp N_{n-1}}{N_n} = w$$

eine ganze Zahl sein.

Hängt man jetzt an die Quotientenreihe a_0, a_1..., a_n, welche sich durch die Entwickelung von $K'_m=K_n$ mit grössten Subquotienten ergeben hat, folgende unendliche Reihe von Quotienten

$$a_{n+1} = \pm(a'_{m+1} + w), \quad a_{n+2} = a'_{m+2}, \quad a_{n+3} = a'_{m+3} \ldots$$

worin bei a_{n+1} das obere oder untere Zeichen gilt, jenachdem in w das obere oder untere Zeichen stattfindet; so ist klar, dass in der unendlichen Reihe a_0, a_1, a_2... alle Quotienten vom zweiten an positiv und $\geqq 1$ sind, mit etwaiger Ausnahme von a_{n+1}, welcher auch $=0$ oder negativ sein kann, ferner, dass von a_{n+2} an alle folgenden Quotienten denen aus der Entwickelung K' von a'_{m+2} an gerechnet gleich sind, endlich dass die Näherungswerthe des aus dieser Quotientenreihe gebildeten Kettenbruchs vom Zeiger n an denen der Entwickelung K' vom Zeiger m an gleich sind, indem man $K_n=K'_m$, $K_{n+1}=K'_{m+1}$ etc. und dem absoluten Werthe nach auch $M_n=M'_m$, $M_{n+1}=M'_{m+1}$

etc. und $N_n = N'_m$, $N_{n+1} = N'_{m+1}$ etc. hat. Da nach Obigem die absoluten Werthe der Zähler M_0, $M_1 \dots M_n$, sowie auch die Zähler M'_m, $M'_{m+1} \dots$ oder M_n, $M_{n+1} \dots$ eine stetig wachsende Zahlenreihe darstellen; so folgt ferner, dass jeder spätere Zähler (und ebenso auch jeder spätere Nenner) der eben bezeichneten unendlichen Reihe M_0, $M_1 \dots M_n$, $M_{n+1} \dots$, absolut genommen, grösser ist, als der vorhergehende. Aus der letzteren Thatsache erkennt man, dass wenn der Quotient a_{n+1} nicht positiv sein sollte, derselbe doch weder $= 0$, noch $= -1$ sein kann, also in diesem Falle $\leqq -2$ sein muss.

Ist also der eben erwähnte Quotient a_{n+1} positiv; so sind sie es vom zweiten an alle, und der Satz, worauf es ankam, ist erwiesen. Wäre jedoch a_{n+1} negativ; so beachte man folgende zwei Hülfssätze.

Wenn die Quotientenreihe eines endlichen Kettenbruchs mit den drei Quotienten a, $-b$, c schliesst, und man setzt für diese drei folgende fünf Quotienten $a-1$, 1, $b-2$, 1, $c-1$; so werden von dem neuen und von dem früheren Kettenbruche die letzten und die vorletzten Näherungswerthe resp. einander identisch sein. Schliesst ferner ein endlicher Kettenbruch mit den drei Quotienten d, o, e und setzt man für diese drei den einzigen Quotienten $d+e$; so werden ebenfalls von dem neuen und von dem früheren Kettenbruche die letzten und die vorletzten Näherungswerthe resp. einander identisch sein. Beide Sätze lassen sich durch das bekannte Bildungsgesetz der Zähler und Nenner der Näherungswerthe (§. 3, III) sehr leicht darthun.

Ist also in der unendlichen Quotientenreihe a_0, $a_1 \dots$ der Quotient a_{n+1} negativ $= -b$; so kann man denselben nebst dem vorhergehenden $a_n = a$ und dem nachfolgenden $a_{n+2} = c$ herausnehmen und durch die obigen fünf Quotienten ersetzen, ohne dass dadurch die tiefer liegenden Quotienten und Näherungswerthe eine Änderung erlitten. Da $a \geqq 1$, $b \geqq 2$, $c \geqq 1$ ist; so kann von den eingeschalteten fünf Quotienten keiner negativ werden. Wol aber kann der erste oder der mittelste oder der letzte $= 0$ werden. Ereignete sich Dies; so kann man nach dem zweiten der obigen beiden Sätze nach und nach jeden Quotienten, welcher $= 0$ ist, nebst dem vorhergehenden d und dem nachfolgenden e ausscheiden, indem man für diese drei den einzigen Quotienten $d+e$ setzt, ohne dass dadurch die späteren Quotienten und Näherungswerthe eine Änderung erlitten.

Hierdurch erhält man in allen Fällen eine unendliche Reihe von Quotienten, welche vom zweiten an positiv sind, von einer gewissen Stelle an mit denen der Entwickelung K' übereinstimmen und einen Kettenbruch darstellen, dessen Näherungswerthe

von jener Stelle an gleich denen von K' sind. Dieser Kettenbruch kann, wie schon vorhin bemerkt, nur die Entwickelung von $K' = K$ nach dem Prinzipe der grössten Subquotienten sein.

Durch das Vorstehende ist also nachgewiesen, dass von einer gewissen Stelle an nicht allein die Quotienten, sondern auch die Näherungswerthe von K und K' gleich sind.

Da nun für K und K' die Grössen P_0, Q_0, Q_{-1} dieselben sind; so folgt aus der Übereinstimmung der Grössen M und N von einer gewissen Stelle an, wegen der Gleichungen (1) und (2) in §. 68, welche sowol für K, als auch für K' gelten, dass auch die absoluten Werthe der Grössen P, Q von der betreffenden Stelle an miteinander vollkommen übereinstimmen. Da die letztern Grössen in der Periode liegen, also nur positiv sein können; so stimmen auch deren Zeichen genau überein, und demnach erhellet aus den Gleichungen (1) und (2) in §. 68, dass die Nummern der Zeiger der übereinstimmenden Grössen aus K und K' nur durch eine paare Differenz sich voneinander unterscheiden können.

VI. Setzt man z. B. in dem ersten Beispiele dieses Paragraphen die bis a_5 ganz willkürliche Entwickelung von $\frac{\sqrt{10}+2}{3}$ nunmehr mit grössten Subquotienten fort; so ergibt sich

$$x_6 = \frac{\sqrt{10}-119}{267} = -1 + \frac{1}{x_7}$$

$$x_7 = \frac{267}{\sqrt{10}+148} = \frac{\sqrt{10}-148}{-82} = 1 + \frac{1}{x_8}$$

$$x_8 = \frac{-82}{\sqrt{10}-66} = \frac{\sqrt{10}+66}{53} = 1 + \frac{1}{x_9}$$

$$x_9 = \frac{53}{\sqrt{10}+13} = \frac{\sqrt{10}-13}{-3} = 3 + \frac{1}{x_{10}}$$

$$x_{10} = \frac{-3}{\sqrt{10}-4} = \frac{\sqrt{10}+4}{2} = 3 + \frac{1}{x_{11}}$$

$$x_{11} = \frac{2}{\sqrt{10}-2} = \frac{\sqrt{10}+2}{3} = 1 + \frac{1}{x_{12}}$$

$$x_{12} = \frac{3}{\sqrt{10}-1} = \frac{\sqrt{10}+1}{3} = 1 + \frac{1}{x_{13}}$$

$$x_{13} = \frac{3}{\sqrt{10}-2} = \frac{\sqrt{10}+2}{2} = 2 + \frac{1}{x_{14}}$$

$$x_{14} = \frac{2}{\sqrt{10}-2} = \frac{\sqrt{10}+2}{3} = x_{11}.$$

Man hat also folgende Fortsetzung der Entwickelung von $\frac{\sqrt{10}+2}{3}$

n	P_n	Q_n	a_n	M_n	N_n
4	-13	3	0	-5	-1
5	13	-53	2	-11	-2
6	-119	267	-1	6	1
7	-148	-82	1	-5	-1
8	66	53	1	1	0
9	-13	-3	3	-2	-1
10	4	2	3	-5	-3
11	2	3	1	-7	-4
12	1	3	1	-12	-7
13	2	2	2	-31	-18
14	2	3	1	-43	-25

Hätte man $\frac{\sqrt{10}+2}{3}$ gleich von vorn herein mit grössten Subquotienten entwickelt; so würde man erhalten haben

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		2		1	0
0	2	3	1	1	1
1	1	3	1	2	1
2	2	2	2	5	3
3	2	3	1	7	4
4	1	3	1	12	7
5	2	2	2	31	18
6	2	3	1	43	25

Die vollständige Übereinstimmung der Periode der Quotienten und der Grössen P, Q in diesen beiden Entwickelungen beginnt resp. bei den Zeigern 11 und 0. Rechnet man die Übereinstimmung dieser periodischen Grössen resp. von den Zeigern 11 und 3 an, welche eine paare Differenz besitzen; so stimmen von hier an auch die Näherungswerthe überein. Dass die Zähler und Nenner in der Einen Entwickelung die entgegengesetzten Zeichen von denen in der andern haben, thut Nichts zur Sache; man konnte, um völlige Übereinstimmung auch in diesen Zeichen zu bewirken, in der Einen Entwickelung $N_{-2} = -1$, $M_{-1} = -1$ setzen (§. 19).

§ 71. Beziehungen zwischen $K = \frac{\sqrt{D}+P_0}{Q_0}$ und $-K = \frac{\sqrt{D}+P_0}{-Q_0}$.

I. Die beiden vorstehenden Grössen K und $-K$, welche sich nur durch das Zeichen von Q_0 unterscheiden, besitzen Ein und dieselbe Periode. Um dies einzusehen, so sei c eine beliebige positive oder negative ganze Zahl. Nimmt man in der Entwickelung von K für die ersten zwei Quotienten a_0, a_1 die Werthe c, 1 und in der Entwickelung von $K' = -K$ für

die ersten drei Quotienten a'_0, a'_1, a'_2 die Werthe $-(c+1)$, 1, 0; so findet man, dass die Grössen P_2, Q_2 aus K mit den Grössen P'_3, Q'_3 aus K' genau übereinstimmen, sodass nun alle Grössen aus K von dem Zeiger 2 an mit den betreffenden Grössen aus K' von dem Zeiger 3 an übereinstimmen.

Es ergibt sich nämlich, wie leicht nachzuweisen ist,

für $K = \frac{\sqrt{D}+P_0}{Q_0}$

n	P_n	Q_n	a_n
-1		Q_{-1}	
0	P_0	Q_0	c
1	P_1	Q_1	1
2	P_2	Q_2	

für $K' = -K = \frac{\sqrt{D}+P_0}{-Q_0}$

n	P_n	Q_n	a_n
-1		$-Q_{-1}$	
0	P_0	$-Q_0$	$-(c+1)$
1	P'_1	Q'_1	1
2	$-P_2$	Q_1	0
3	P_2	Q_2	

Setzt man nun die Entwickelung von $x_2 = x'_3 = \frac{\sqrt{D}+P_2}{Q_2}$ mit grössten Subquotienten fort; so gibt Dies nach dem vorhergehenden Paragraphen dieselbe Periode, wie wenn man gleich von vorn herein K oder $K' = -K$ mit solchen Quotienten entwickelt hätte. Die Perioden von K und $-K$ sind also gleich und auch die Näherungswerthe von einer gewissen Stelle an, abgesehen von deren Zeichen.

Hiernach haben also auch $\sqrt{D}$ und $-\sqrt{D}$ d. i. $\frac{\sqrt{D}+0}{1}$ und $\frac{\sqrt{D}+0}{-1}$ stets gleiche Perioden.

Als Beispiel wollen wir, nachdem im vorhergehenden Paragraphen $K = \frac{\sqrt{10}+2}{3}$ entwickelt ist, $K' = \frac{\sqrt{10}+2}{-3}$ in einen Kettenbruch mit grössten Subquotienten verwandeln. Dies gibt

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-2		1	0
0	2	-3	-2	-2	1
1	4	2	3	-5	3
2	2	3	1	-7	4
3	1	3	1	-12	7
4	2	2	2	-31	18

II. Aus dem gegenwärtigen Satze folgt die wichtige Vervollständigung des Satzes in §. 65 über die **Minimalwerthe** der Grössen Q. Man kann jetzt nämlich begreifen, dass wenn es ein **negatives** Q gibt, dessen absoluter Betrag $\leq a$ ist, dieser Betrag nothwendig auch in der **Periode** der Grössen vorkommen muss. Denn bezeichnet Q_n eine positive, P_n aber eine

positive oder negative Grösse; so führt die fernere Entwickelung von $x_n = \frac{\sqrt{D}+P_n}{-Q_n}$ zu derselben Periode, zu welcher die Entwickelung von $-x_n = \frac{\sqrt{D}+P_n}{Q_n}$ führen würde. Ist nun nach der Voraussetzung $Q_n \leqq a$; so liegt nach §. 65 Q_n in der Periode der Grössen Q, welche die Entwickelung von $-x_n$ bilden, und mithin auch in der Periode von x_n.

Aber auch die Grösse $Q_{-1} = \frac{D - P_0^2}{Q_0}$ ist dem vorstehenden Gesetze unterworfen, und es muss ihr absoluter Betrag, wenn er $\leqq a$ ist, jedenfalls in der Periode erscheinen. Denn nimmt man als ersten Quotienten in der Entwickelung von $K = \frac{\sqrt{D}+P_0}{Q_0}$ den Werth $a_0 = 0$; so wird $P_1 = a_0 Q_0 - P_0 = -P_0$ und mithin $Q_1 = \frac{D - P_1^2}{Q_0} = \frac{D - P_0^2}{Q_0} = Q_{-1}$. Von der ferneren Entwickelung der Grösse $x_1 = \frac{\sqrt{D}+P_1}{Q_1} = \frac{\sqrt{D}-P_0}{Q_{-1}}$ gilt aber das vorstehende Gesetz.

Hieraus ist nun klar, dass man durch keinerlei willkürliche Quotienten bewirken kann, dass in der Entwickelung von K unter den numerischen Werthen von Q solche auftreten, welche $\leqq a$ wären und nicht auch in der Periode vorkämen.

III. Wir machen noch auf Folgendes aufmerksam. Durch die obige Entwickelung von K' mit den ersten drei willkürlichen Quotienten $-(c+1)$, 1, 0 wird erreicht, dass die Zeiger der beiden Glieder, bei welchen die Entwickelungen von K und K' in Übereinstimmung treten, sich um den Werth 1, also um eine unpaare Differenz unterscheiden. Da nun nach §. 70 die Zeiger der übereinstimmenden Glieder in jeden zwei beliebigen Entwickelungen derselben Grösse wie K oder K' stets eine paare Differenz besitzen; so folgt, dass, wie man auch $K = \frac{\sqrt{D}+P_0}{Q_0}$ und $K' = \frac{\sqrt{D}+P_0}{-Q_0}$ entwickeln möge, immer an den Stellen, wo die Übereinstimmung Beider eintritt, die betreffenden Zeiger aus beiden Entwickelungen durch eine unpaare Differenz sich unterscheiden werden.

IV. Noch anschaulicher wird die Überführung der Entwickelung von $K = \frac{\sqrt{D}+P_0}{Q_0}$ auf die von $K' = \frac{\sqrt{D}+P_0}{-Q_0}$ oder

umgekehrt durch die Bemerkung, dass wenn man in der Entwickelung von K für die ersten drei Quotienten die Werthe $a_0, a_1, a_2 = 1, -1, 1$ annimmt, sofort beim Zeiger 3

$$x_3 = \frac{\sqrt{D}+P_0}{-Q_0} = K' \text{ also } P_3 = P_0 \text{ und } Q_3 = -Q_0$$

auch $Q_2 = -Q_{-1}$ wird. Dies ist durch die Formeln (1) und (5) des §. 61 mit Leichtigkeit zu konstatiren. So hat man z. B.

für $K = \frac{\sqrt{10}+2}{3}$

n	P_n	Q_n	a_n
-1		2	
0	2	3	1
1	1	3	-1
2	-4	-2	1
3	2	-3.	

oder für $K = \frac{\sqrt{10}+2}{-3}$

n	P_n	Q_n	a_n
-1		-2	
0	2	-3	1
1	-5	5	-1
2	0	2	1
3	2	3	

§. 72. Einfluss des Werthes von P_0 auf die Entwickelung von K.

I. Es ist klar, dass wenn in dem Ausdrucke $K = \frac{\sqrt{D}+P_0}{Q_0}$ der Werth von P_0 um irgend ein Vielfaches von Q_0 vermehrt oder vermindert wird, Dies nur einen Einfluss auf den ersten Quotienten a_0 und auf die zurückliegende Grösse Q_{-1}, sonst aber auf keine Grösse der Entwickelung von K haben kann.

Man hat nämlich, indem w irgend eine positive oder negative ganze Zahl darstellt,

$$\text{wenn } K = \frac{\sqrt{D}+P_0}{Q_0} = a_0 + \frac{1}{x_1}, \text{ also } Q_{-1} = \frac{D-P_0^2}{Q_0} \text{ ist,}$$

$$K' = \frac{\sqrt{D}+P_0+wQ_0}{Q_0} = \frac{\sqrt{D}+P_0}{Q_0} + w = (a_0+w) + \frac{1}{x_1}$$

$$Q'_{-1} = \frac{D-(P_0+wQ_0)^2}{Q_0} = \frac{D-P_0^2}{Q_0} - 2wP_0 - w^2 Q_0$$
$$= Q_{-1} - 2wP_0 - w^2 Q_0$$

also

(1) $a'_0 = a_0 + w$

(2) $Q'_{-1} = Q_{-1} - 2wP_0 - w^2 Q_0$

Sieht man also von dem ersten Quotienten oder der Grösse Q vom Zeiger -1 ab; so können unter den Werthen von K, in welchen D und Q_0 konstant erhalten werden, nur solche eine verschiedene Entwickelung ergeben, in welchen P_0 positiv und $< Q_0$ ist, indem man ja, wenn $P_0 \geq Q_0$ wäre, von P_0 ein so grosses Vielfaches wQ_0 der Grösse Q_0 trennen könnte, dass an der Stelle jener Grösse ein Betrag $< Q_0$ stehen bliebe. So hat man $\frac{\sqrt{10}+17}{3} = \frac{\sqrt{10}+2}{3} + 5$ oder $\frac{\sqrt{10}-17}{3} = \frac{\sqrt{10}+1}{3} - 6$

Wenn man übrigens für P_0 auch negative Werthe zulassen will; so ist klar, dass man durch Absonderung des betreffenden Vielfachen von Q_0 es stets dahin bringen kann, dass der numerische Werth der an der Stelle von P_0 stehen bleibenden Zahl $\leqq \frac{1}{2} Q_0$ ist. So hat man $\frac{\sqrt{10}+17}{3}=\frac{\sqrt{10}-1}{3}+6$.

II. Betrachten wir jetzt die Beziehungen zwischen den Entwickelungen von

$$K=\frac{\sqrt{D}+P_0}{Q_0} \text{ und } K'=\frac{\sqrt{D}-P_0}{Q_0}$$

worin also P_0 und P'_0 entgegengesetzte Zeichen haben. Setzen wir die Entwickelung von $K=[a_0, a_1, a_2 \ldots]$ als bekannt und die von K' als gesucht voraus; so erhellet sofort aus den Reihen (1), (2) und (3), (4) des §. 61, dass wenn man in der Entwickelung von K' statt a'_0, a'_1, $a'_2 \ldots$ als willkürliche Quotienten die entgegengesetzten Werthe von a_0, a_1, $a_2 \ldots$ nimmt, also $K'=[-a_0, -a_1, -a_2 \ldots]$ setzt, hierdurch resp. $P'_0, P'_1, P'_2 \ldots = -P_0, -P_1, -P_2 \ldots$ dagegen $Q'_0, Q'_1, Q'_2 \ldots = Q_0, Q_1, Q_2 \ldots$ werden. Es wird sich also ergeben

für $K=\frac{\sqrt{D}+P_0}{Q_0}$				für $K'=\frac{\sqrt{D}-P_0}{Q_0}$			
n	P_n	Q_n	a_n	n	P'_n	Q'_n	a'_n
-1		Q_{-1}		-1		Q_{-1}	
0	P_0	Q_0	a_0	0	$-P_0$	Q_0	$-a_0$
1	P_1	Q_1	a_1	1	$-P_1$	Q_1	$-a_1$
2	P_2	Q_2	a_2	2	$-P_2$	Q_2	$-a_2$
3	P_3	Q_3	a_3	3	$-P_3$	Q_3	$-a_3$

Wir machen darauf aufmerksam, dass diese Entwickelung von K' mit willkürlichen Quotienten, obgleich sie ebenso periodisch ist, wie die von K, doch keineswegs eine konvergente ist, indem die Fehler in jedem Quotienten im Allgemeinen mehr als Eine Einheit betragen. Demnach nähern sich die Näherungsbrüche von K' in der vorstehenden Entwickelung keineswegs dem wahren Werthe dieser Grösse; man erkennt vielmehr, dass dieselben nach dem absoluten Werthe gleich und nach dem Zeichen entgegengesetzt den Näherungsbrüchen von K sind.

Diese Operation zeigt aber, dass man im Stande sei, die Entwickelung von K' mit jedem Gliede $x_n=\frac{\sqrt{D}+P_n}{Q_n}$ der Entwickelung von K dergestalt in Übereinstimmung zu bringen, dass sich nur die Grössen P_n durch das Zeichen unterscheiden, sodass man also $x'_n=\frac{\sqrt{D}+P'_n}{Q'_n}=\frac{\sqrt{D}-P_n}{Q_n}$ hat. Von jedem dieser Glieder kann man, wenn man will, die Entwickelung von

K' mit grössten Subquotienten weiterführen, also in eine konvergente übergehen lassen.

III. Erwägt man nun, dass allgemein

(3) $$\frac{\sqrt{D}-P_n}{Q_n}=\frac{\sqrt{D}+P_n}{Q_n}-\frac{2P_n}{Q_n} \text{ also}$$

$$x'_n=x_n+\frac{2P_n}{Q_n}$$

ist; so leuchtet ein, dass die mit grössten Subquotienten erzielte Periode von K' in alle den Fällen gleich der von K ist, wo in der Entwickelung von K zwei zusammengehörige Grössen P_n, Q_n vorkommen, für welche $\frac{2P_n}{Q_n}$ eine ganze Zahl w oder

(4) $$\frac{2P_n}{Q_n}=w$$

ist, indem man dann sofort $x'_n=x_n+w$ also $a'_n=a_n+w$ und ferner resp.

$$P'_{n+1},\ P'_{n+2},\ P'_{n+3}\ldots=P_{n+1},\quad P_{n+2},\ P_{n+3}\ldots$$
$$Q'_{n+1},\ Q'_{n+2},\ Q'_{n+3}\ldots=Q_{n+1},\quad Q_{n+2},\ Q_{n+3}\ldots$$
$$a'_{n+1},\ a'_{n+2},\ a'_{n+3}\ldots=(a_n+w),\ a_{n+2},\ a_{n+3}\ldots$$

hat. Unter solchen Umständen kann also ohne Weiteres eine Entwickelung von K in eine Entwickelung von K' umgeschrieben werden, wobei jedoch die Letztere bis zum Zeiger n nicht die grössten Subquotienten enthält.

Die Bedingung (4) kann schon für den Zeiger 0 erfüllt sein. Dies wird offenbar jederzeit der Fall sein, wenn $Q_0=1$ oder $=2$ ist. Es haben also

$$\sqrt{D}+P_0 \text{ und } \sqrt{D}-P_0 \text{ sowie}$$
$$\frac{\sqrt{D}+P_0}{2} \text{ und } \frac{\sqrt{D}-P_0}{2}$$

stets gleiche Perioden.

So ist z. B. $\frac{\sqrt{11}+3}{2}=[3,\ 6,\ 3,\ 6\ldots]$ und $\frac{\sqrt{11}-3}{2}$ $=[0,\ 6,\ 3,\ 6,\ 3,\ 6\ldots]$

Die Bedingung (4) ist ferner dann immer erfüllt, wenn unter den Grössen Q der Entwickelung von K irgendwo ein Werth $Q_n=\pm1$ oder $Q_n=\pm2$ vorkommt.

Dass also z. B. $\frac{\sqrt{10}+2}{3}$ und $\frac{\sqrt{10}-2}{3}$ gleiche Perioden haben, erkennt man aus der in §. 70, VI mitgetheilten Entwickelung der ersteren Grösse, indem man daselbst $P_2=2$, $Q_2=2$ also $\frac{2P_2}{Q_2}=\frac{2.2}{2}=2=w$ hat. In der That ist $\frac{\sqrt{11}-2}{3}=$ $[0,\ 2,\ 1,\ 1,\ 2,\ 1,\ 1,\ 2\ldots]$.

Die Bedingung (4) ist nach §. 64 in alle den Fällen erfüllt, wo die Periode von K symmetrisch ist. Es leuchtet also ein, dass für jede Grösse $\frac{\sqrt{D}+P_0}{Q_0}$, welche eine symmetrische Periode besitzt, auch $\frac{\sqrt{D}-P_0}{Q_0}$ dieselbe symmetrische Periode besitzen wird.

IV. Wir bemerken noch, dass wenn man in der Entwikkelung von $K' = \frac{\sqrt{D}-P_0}{Q_0}$ den ersten Quotienten $a'_0 = 0$ nimmt, sich

$$x'_0 = \frac{\sqrt{D}-P_0}{Q_0} = 0 + \frac{1}{x'_1}$$

$$x'_1 = \frac{\sqrt{D}+P_0}{Q_{-1}}, \text{ also}$$

$$P'_1 = P_0, \quad Q'_1 = Q_{-1}$$

ergibt. Hieraus erhellet, dass

$$\frac{\sqrt{D}-P_0}{Q_0} \text{ und } \frac{\sqrt{D}+P_0}{Q_{-1}}, \text{ worin}$$

$$Q_0\, Q_{-1} = D - P_0^2$$

ist, stets dieselbe Periode haben. Dasselbe gilt von

$$\frac{\sqrt{D}+P_0}{Q_0} \text{ und } \frac{\sqrt{D}-P_0}{Q_{-1}}$$

Demnach haben z. B. für $19 - 3^2 = 2 \,.\, 5$ die beiden Grössen $\frac{\sqrt{19}-3}{2}$ und $\frac{\sqrt{19}+3}{5}$ oder auch die beiden Grössen $\frac{\sqrt{19}+3}{2}$ und $\frac{\sqrt{19}-3}{5}$ gleiche Perioden.

V. Ferner ist klar, dass die obigen Bedingungen, unter welchen

$$\frac{\sqrt{D}+P_0}{Q_0} \text{ und } \frac{\sqrt{D}-P_0}{Q_0}$$

gleiche Perioden haben, dieselben sind, unter welchen

$$\frac{\sqrt{D}+P_0}{Q_0} \text{ und } \frac{\sqrt{D}+P_0}{Q_{-1}}$$

gleiche Perioden besitzen. Wenn sich Letzteres ereignet, haben offenbar alle vier Grössen

$$\frac{\sqrt{D}+P_0}{Q_0},\ \frac{\sqrt{D}-P_0}{Q_0},\ \frac{\sqrt{D}+P_0}{Q_{-1}},\ \frac{\sqrt{D}-P_0}{Q_{-1}}$$

gleiche Perioden.

Die letzteren Beziehungen sind auch gültig, wenn man für die Zeiger 0 und -1 allgemein n und $n-1$ setzt. Nimmt man nämlich an irgend einer Stelle den Quotienten $a_n = 0$; so folgt auf

$$x_n = \frac{\sqrt{D}+P_n}{Q_n} = 0 + \frac{1}{x_{n+1}} \text{ der Werth}$$

$$x_{n+1} = \frac{\sqrt{D}-P_n}{Q_{n-1}} \text{ also}$$

$$P_{n+1} = -P_n, \quad Q_{n+1} = Q_{n-1}$$

VI. Schliesslich machen wir noch auf folgende Beziehungen aufmerksam. Wenn man in $K = \frac{\sqrt{D}+P_0}{Q_0}$ gleichzeitig die Zeichen von P_0 und Q_0 umkehrt; so kann man für

$$K'' = \frac{\sqrt{D}-P_0}{-Q_0}, \text{ dessen Werth auch } = \frac{-\sqrt{D}+P_0}{Q_0}$$

ist, die Quotienten $a_0, a_1 \ldots$ von K beibehalten. Dies gibt nach §. 61

$$\begin{array}{ll} a''_0,\ a''_1,\ a''_2 \ldots = & a_0,\ a_1,\ a_2 \ldots \\ P''_0,\ P''_1,\ P''_2 \ldots = & -P_0, -P_1, -P_2 \ldots \\ Q''_{-1},\ Q''_0,\ Q''_1,\ Q''_2 \ldots = & -Q_{-1}, -Q_0, -Q_1, -Q_2 \ldots \end{array}$$

wobei natürlich $a_0, a_1 \ldots$ nicht die grössten Subquotienten von K'' darstellen.

Entwickelt man K'' nach grössten Subquotienten; so ergibt sich nicht unbedingt dieselbe Periode, wie für K. Denn wenn auch stets $\frac{\sqrt{D}-P_0}{-Q_0}$ und $\frac{\sqrt{D}-P_0}{Q_0}$ gleiche Perioden haben; so lässt sich Dasselbe doch nicht allgemein von $\frac{\sqrt{D}-P_0}{Q_0}$ und $\frac{\sqrt{D}+P_0}{Q_0}$, also nicht von K und K'' sagen. Jenachdem man also in $\frac{\pm\sqrt{D}+P_0}{Q_0}$ das obere oder untere Zeichen nimmt, kann eine Entwickelung nach grössten Subquotienten eine andere Periode ergeben.

§. 73. *Kombination zweier Entwickelungen K und K', welche gleiche Perioden besitzen.*

I. Man habe folgende zwei Entwickelungen, denen Ein und dieselbe Determinante D zu Grunde liege, in welchen aber die Quotienten ganz beliebige Werthe haben mögen.

$$K=\frac{\sqrt{D}+P_0}{Q_0}$$

m	P_m	Q_m	a_m
-1		Q_{-1}	
0	P_0	Q_0	a_0
1	P_1	Q_1	a_1
2	P_2	Q_2	a_2
$\vdots$			
$m-1$	P_{m-1}	Q_{m-1}	a_{m-1}
m	P_m	Q_m	a_m
$m+1$	P_{m+1}	Q_{m+1}	a_{m+1}
$m+2$	P_{m+2}	Q_{m+2}	a_{m+2}

$$K'=\frac{\sqrt{D}+P'_0}{Q'_0}$$

n	P'_n	Q'_n	a'_n
-1		Q'_{-1}	
0	P'_0	Q'_0	a'_0
1	P'_1	Q'_1	a'_1
2	P'_2	Q'_2	a'_2
$\vdots$			
$n-1$	P'_{n-1}	Q'_{n-1}	a'_{n-1}
n	P'_n	Q'_n	a'_n
$n+1$	P'_{n+1}	Q'_{n+1}	a'_{n+1}
$n+2$	P'_{n+2}	Q'_{n+2}	a'_{n+2}

Angenommen, in diesen beiden Entwickelungen seien zwei Glieder wie x_m und x'_n identisch, also $\frac{\sqrt{D}+P_m}{Q_m}=\frac{\sqrt{D}+P'_n}{Q'_n}$; so muss man haben

(1) $P_m=P'_n,\quad Q_m=Q'_n,\quad Q_{m-1}=Q'_{n-1}$

Behält man von der Entwickelung K die über dem gebrochenen Striche liegenden Grössen bei, setzt für den Quotienten a_m den Werth null und lässt unter dem horizontalen Striche die in der Entwickelung K' über dem gebrochenen Striche stehenden Grössen in umgekehrter Reihenfolge und indem man die Grössen P' und a' mit entgegengesetzten Zeichen nimmt, folgen, sodass man also setzt:

(2) $a_m=0$

(3) $a_{m+1},\ a_{m+2},\ a_{m+3}\ldots=-a'_{n-1},\ -a'_{n-2},\ -a'_{n-3}\ldots$

(4) $Q_{m+1},\ Q_{m+2},\ Q_{m+3}\ldots=\quad Q'_{n-1},\quad Q'_{n-2},\quad Q'_{n-3}\ldots$

(5) $P_{m+1},\ P_{m+2},\ P_{m+3}\ldots=-P'_n,\ -P'_{n-1},\ -P'_{n-2}\ldots$

so erhält man die nachstehende Entwickelung von K:

$$K=\frac{\sqrt{D}+P_0}{Q_0}$$

m	P_m	Q_m	a_m	M_m	N_m
-2				0	1
-1		Q_{-1}		1	0
0	P_0	Q_0	a_0	M_0	N_0
1	P_1	Q_1	a_1	M_1	N_1
2	P_2	Q_2	a_2	M_2	N_2
$\vdots$					
$m-1$	P_{m-1}	Q_{m-1}	a_{m-1}	M_{m-1}	N_{m-1}
m	P_m	Q_m	0	M_{m-2}	N_{m-2}
$m+1$	$-P'_n$	Q'_{n-1}	$-a'_{n-1}$	.	.
$m+2$	$-P'_{n-1}$	Q'_{n-2}	$-a'_{n-2}$	.	.
$m+3$	$-P'_{n-2}$	Q'_{n-3}	$-a'_{n-3}$	.	.
$\vdots$					
$m+n-2$	$-P'_3$	Q'_2	$-a'_2$		
$m+n-1$	$-P'_2$	Q'_1	$-a'_1$		
$m+n$	$-P'_1$	Q'_0	$-a'_0$		
$m+n+1$	$-P'_0$	Q'_{-1}			

Die Richtigkeit dieser Zusammenfügung, welche wir eine Kombination von K und K' nennen und durch die Formel

(6) $K(m)$ *komb.* $K'(n)$

bezeichnen wollen, ist mit Leichtigkeit durch die Grundformeln (1), (2) und (3), (4) des §. 61 darzuthun.

II. In der vorstehenden Kombination ist der obere Theil von K' in seiner ganzen Totalität bis zu dem obersten Werthe Q'_{-1} der Grössen Q' mit der Entwickelung von K vereinigt, und Dies hat zur Folge, dass der Schluss

$$(7) \quad \begin{cases} m+n-1 & -P'_2 & Q'_1 & a'_1 \\ m+n & -P'_1 & Q'_0 & a'_0 \\ m+n+1 & -P'_0 & Q'_{-1} & \end{cases}$$

wird. Die Grösse Q'_0 erscheint also in dieser Entwickelung von K bei dem Zeiger $m+n$, und die Grösse Q'_{-1} bei dem Zeiger $m+n+1$.

Wenn man will, kann man offenbar diese Anhängung bei jedem beliebigen Zeiger abbrechen. Wir werden dieselbe bei der Anwendung auf die unbestimmten Gleichungen immer bei dem vorletzten Zeiger $m+n$ abbrechen, sodass Q'_0 in der Reihe der Q und $-a'_1$ in der Reihe der Quotienten die letzte Grösse ist, was folgenden Schluss ergibt

$$(8) \quad \begin{cases} m+n-1 & -P'_2 & Q'_1 & a'_1 \\ m+n & -P'_1 & Q'_0 & \end{cases}$$

III. Die Bedingung (1), worauf sich die vorstehende Kombination gründet, setzt voraus, dass K und K', wenn sie mit grössten Subquotienten entwickelt werden, gleiche Perioden haben, und umgekehrt ist klar, dass zwei Entwickelungen mit gleichen Perioden an jeden zwei identischen Stellen dieser Perioden in vorstehender Weise kombinirt werden können.

Als Beispiel wollen wir folgende zwei Entwickelungen nehmen.

$$K = \frac{\sqrt{10}+2}{3} \qquad K' = \frac{\sqrt{10}-12}{2}$$

m	P_m	Q_m	a_m
-1		2	
0	2	3	1
1	1	3	1
2	2	2	2
3	2	3	1
4	1	3	1
5	2	2	2

n	P_n	Q_n	a_n
-1		-67	
0	-12	2	-5
1	2	3	1
2	1	3	1
3	2	2	2
4	2	3	1
5	1	3	1
6	2	2	2

Hier kann man offenbar

jeden Werth von K (0), (3), (6) ... mit jedem Werthe von K' (1), (4), (7) ...
„ „ „ K (1), (4), (7) ... „ „ „ „ K' (2), (5), (8) ...
„ „ „ K (2), (5), (8) ... „ „ „ „ K' (3), (6), (9) ...

kombiniren. Für K (3) *komb.* K' (4) hat man

m	P_m	Q_m	a_m	M_m	N_m
-2				0	1
-1		2		1	0
0	2	3	1	1	1
1	1	3	1	2	1
2	2	2	2	5	3
3	2	3	0	2	1
4	-2	2	-2	1	1
5	-2	3	-1	1	0
6	-1	3	-1	0	1
7	-2	2	5	1	5
8	12				

IV. Durch dieses Verfahren ist es leicht, wenn zwei Grössen Q_0 und Q'_0 bekannt sind, für welche sich $K=\frac{\sqrt{D}+P_0}{Q_0}$ und $K'=\frac{\sqrt{D}+P'_0}{Q'_0}$ als zwei Entwickelungen mit gleichen Perioden darstellen lassen, eine Entwickelung von K zu bilden, in welcher die Grösse Q'_0 in der Reihe der Q erscheint.

Umgekehrt ist hieraus und aus §. 72 klar, dass jede Grösse Q'_0, welche fähig ist, in irgend einer Entwickelung von $K=\frac{\sqrt{D}+P_0}{Q_0}$ unter der Reihe der Q zu erscheinen, von der Art sein muss, dass zu ihr eine Grösse P'_0 mit einem numerischen Werthe $\leqq \frac{1}{2}\, Q'_0$ gefunden werden kann, vermittelst welcher $K'=\frac{\sqrt{D}+P'_0}{Q'_0}$ ein Ausdruck wird, der mit $K=\frac{\sqrt{D}+P_0}{Q_0}$ eine gleiche Periode besitzt.

V. Nimmt man bei der obigen Kombination $K'=K$; so kann man nach der Formel $K(n)$ *komb.* $K(n)$ in der Entwickelung von K von jedem Gliede aus rückwärts schreiten, und zwar nach folgendem Schema, wobei sich auch die früheren Näherungswerthe reproduziren.

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		Q_{-1}		1	0
0	P_0	Q_0	a_0	M_0	N_0
1	P_1	Q_1	a_1	M_1	N_1
.					
.					
.					

(Fortsetzung auf der folgenden Seite.)

⋮					
$n-1$	P_{n-1}	Q_{n-1}	a_{n-1}	M_{n-1}	N_{n-1}
n	P_n	Q_n	0	M_{n-2}	N_{n-2}
$n+1$	$-P_n$	Q_{n-1}	$-a_{n-1}$	M_{n-3}	N_{n-3}
$n+2$	$-P_{n-1}$	Q_{n-2}	$-a_{n-2}$	M_{n-4}	N_{n-4}
⋮					
$2n-2$	$-P_3$	Q_2	$-a_2$	M_0	N_0
$2n-1$	$-P_2$	Q_1	$-a_1$	1	0
$2n$	$-P_1$	Q_0	$-a_0$	0	1
$2n+1$	$-P_0$	Q_{-1}	0	1	0
$2n+2$	P_0	Q_0			

In dieser Kombination, welcher wir am Ende noch den Quotienten 0 hinzugefügt haben, stellt sich die Grösse Q_0 zuerst bei dem Zeiger $2n$ wieder ein. Bei dem Zeiger $2n+1$ ergeben sich die Endformeln des vorhergehenden Paragraphen. Bei dem Zeiger $2n+2$ stellen sich die beiden Grössen P_0, Q_0, welche den Anfang der Entwickelung von K bilden, zusammen ein. Setzt man in dem angehängten Theile statt eines Quotienten wie $-a_{n-r-1}$ den Werth 0; so erhält man beim Zeiger $n+r+2$ die beiden Grössen P_{n-r}, Q_{n-r}, welche ein zusammengehöriges Paar aus der ursprünglichen Entwickelung von K bilden. Demnach kann man nicht allein jedes spätere Paar solcher Grössen, wie P_{n+r}, Q_{n+r}, sondern auch jedes frühere Paar, wie P_{n-r}, Q_{n-r}, als in der Fortsetzung der Entwickelung unterhalb des Paares P_n, Q_n liegend betrachten, wenn man im letzteren Falle auf den Quotienten a_{n-1} die Quotienten $0, -a_{n-1}, -a_{n-2} \ldots -a_{n-r}, 0$ folgen lässt.

VI. Von jetzt an werden wir unter der Kombination (6) der beiden mit gleichen Perioden begabten Entwickelungen K und K', wodurch eine neue Entwickelung von K gewonnen wird, also unter der Kombination $K(m)$ *komb.* $K'(n)$ im engeren Sinne den Werth des Kettenbruchs

$$[a_0, a_1, a_2 \ldots a_{m-1}, 0, -a'_{n-1}, -a'_{n-2} \ldots -a'_1]$$

verstehen, worin der Schluss nach der Formel (8) gebildet, also $-a'_1$ der letzte angehängte Quotient ist, welchem in der Kombination der Zeiger $m+n-1$ zukommt, sodass in der neuen Entwickelung von K der Werth Q'_0 in der Reihe der Grössen Q bei dem Zeiger $m+n$ erscheint.

Man hat nun folgende wichtige Sätze. Wenn r die Gliederzahl der gleichen Perioden von K und K' bezeichnet; so ist die obige Kombination (6) auch gleich der folgenden

(9) $$K(m+vr) \text{ komb. } K'(n+vr)$$

worin v irgend eine willkürliche positive ganze Zahl bedeutet. Denn offenbar wird die letztere Kombination erhalten, wenn

man statt des Quotienten 0 in der Kombination (6) die Quotientenreihe

$$a_m, a_{m+1} \ldots a_{m+vr-1}, 0, -a_{m+vr-1} \ldots -a_{m+1}, -a_m$$

einschaltet. Die zweite Hälfte der Quotienten dieser Reihe reproduzirt aber, wie man schon sub V gesehen hat, die Näherungswerthe der ersten Hälfte; sodass, angekommen bei den beiden letzten Quotienten $-a_{m+1}$, $-a_m$ dieser Reihe resp. die beiden Näherungswerthe K_{m-1}, K_{m-2} reproduzirt sind.

Die nämlichen beiden Näherungswerthe in der nämlichen Reihenfolge entstehen nun ebenfalls in der Kombination (6) durch die beiden Quotienten a_{n-1}, 0. Hieraus folgt, dass die fernere Fortsetzung sowol der Kombination (6), als auch die der Kombination (9) durch die letzten Quotienten von $-a'_{n-1}$ bis $-a'_1$ genau dieselben Näherungswerthe hervorbringen muss, dass also beide Kombinationen einander gleich sind.

Sowie die Vermehrung der Zeiger m und n in (6) um Ein und dasselbe Vielfache der Gliederzahl der Periode ohne Einfluss auf den Werth der Kombination ist; ebenso ist es die Verminderung der Zeiger m und n um ein solches Vielfaches, wofern nur die neuen Zeiger $m-vr$ und $n-vr$ in K, und in K' die obere Gränze der Perioden nicht überschreiten.

Auch ist klar, dass man unbeschadet des Werthes der Kombination (6) die Zeiger m und n um jeden beliebigen positiven ganzen Werth w vermehren oder vermindern kann, wofern nur bei der Verminderung in K oder in K' die obere Gränze der übereinstimmenden Glieder (welche zuweilen noch oberhalb der Perioden liegen) nicht überschritten wird.

VII. Sucht man also alle möglichen verschiedenen Kombinationen von K und K'; so erhält man dieselben, indem man zunächst für m und n die Zeiger von irgend zwei in den Perioden liegenden Stellen aus K und K' nimmt, welche die Bedingungen (1) erfüllen, und alsdann folgende zwei Reihen von Kombinationen bildet:

(10) $K(m), (m+r), (m+2r) \ldots$ *komb.* $K'(n)$

(11) $K(m)$ *komb.* $K'(n), (n+r), (n+2r) \ldots$

In diesen beiden Reihen sind nur die ersten Kombinationen $K(m)$ *komb.* $K'(n)$ einander gleich.

So würden in dem obigen Beispiele alle verschiedenen Kombinationen durch die beiden Reihen

$K(0), (3), (6) \ldots$ *komb.* $K'(1)$ und

$K(0)$ *komb.* $K'(1), (4), (7) \ldots$

vollständig dargestellt sein.

Der nähere Zusammenhang zwischen den beiden Reihen von Kombinationen (10), (11) wird in §. 84 erläutert werden.

Wir bemerken noch, dass offenbar

$$K(m) \text{ komb. } K'(0) = K(m)$$

ist, dass also durch die Anhängung von $K'(0)$ an $K(m)$ der Werth von $K(m)$ nicht geändert wird.

VIII. Aus Vorstehendem erkennt man, dass zwei Entwickelungen K und K', in denen von gewissen Zeigern m und n an die Glieder übereinstimmen, mehr als Eine, und zwar unendlich viele verschiedene Kombinationen nur in der Voraussetzung ergeben können, dass jene Entwickelungen periodisch seien. Wären sie nicht periodisch, gleichviel ob sie eine unendliche oder endliche Länge besässen; so würden alle jene Kombinationen offenbar immer die nämlichen Werthe darstellen, sodass es alsdann eigentlich nur Eine Kombination zwischen K und K' gäbe. Diese Bemerkung hat Wichtigkeit für den in §. 87 ff. zu untersuchenden Fall, wo die Determinante D ein vollständiges Quadrat ist.

Ausserdem ist klar, dass wenn K und K' zwar unendlich und periodisch, aber doch von der Beschaffenheit wären, dass die Periode zweigliedrig und alle Quotienten in der Periode den Werth null besässen, die unendliche Mannichfaltigkeit des Anschlusses in den Abständen verschiedener Perioden doch zu keinen verschiedenen Kombinationen führen würde, indem je zwei unmittelbar aufeinander folgende Quotienten wie $a_n = 0$, $a_{n+1} = 0$ stets dieselben vorhergehenden Näherungswerthe regelmässig wiedererzeugen würden, was aus dem Schema

$$\begin{array}{ccc} & M_{n-2} & N_{n-2} \\ & M_{n-1} & N_{n-1} \\ 0 & M_{n-2} & N_{n-2} \\ 0 & M_{n-1} & N_{n-1} \end{array}$$

erhellet. Also auch in einem solchen Falle würde nur von einer einzigen Kombination zwischen K und K' die Rede sein können. Diese Bemerkung ist von Wichtigkeit für den in §. 94 ff. zu untersuchenden Fall, wo die Determinante D negativ ist.

§. 74. *Bedeutung der Formeln des §. 68 für die unbestimmten Gleichungen vom zweiten Grade.*

I. Wenn in der Gl. (2) des §. 68, welche

$$(1) \quad Q_0 M_{n-1}^2 - 2P_0 M_{n-1} N_{n-1} - Q_{-1} N_{n-1}^2 = (-1)^n Q_n$$

ist, die Grössen Q_0, P_0, Q_{-1} und $(-1)^n Q_n$ wie vier gegebene positive oder negative ganze Zahlen, dagegen M_{n-1} und N_{n-1} wie zwei gesuchte ganze Zahlen, welche relativ prim sind, angesehen werden; so entspricht Dies einem gewissen Falle der Auflösung der unbestimmten Gleichungen vom zweiten Grade mit zwei Unbekannten. Hierdurch erhält jene

Formel für die unbestimmte Analytik eine besondere Wichtigkeit. Den Schlüssel zur Verwendung jener Formel in der bezeichneten Absicht, was den Gegenstand des fünften Abschnittes ausmacht, liefert folgende Betrachtung.

II. Wenn P_0, Q_0, Q_{-1} bekannte Zahlen sind; so ergibt sich aus der Beziehung $Q_{-1} = \frac{D - P_0^2}{Q_0}$ der Werth der Determinante D in der Form

(2) $$D = P_0^2 + Q_0\, Q_{-1}$$

Dieser Werth von D ist stets eine ganze Zahl, und wir setzten vorläufig auch voraus, dass er positiv und kein vollkommenes Quadrat sei. Ausserdem entspricht er der Bedingung (2) in §. 59, wonach $Q_{-1} = \frac{D - P_0^2}{Q_0}$ eine ganze Zahl sein soll.

III. Nun ist klar, dass jede zwei relative Primzahlen M_{n-1}, N_{n-1}, welche die Gl. (1) erfüllen, nebst der Zahl $(-1)^n\, Q_n$, in der schon mehrfach erläuterten Weise zum Vorschein kommen müssen, wenn man den Ausdruck

(3) $$K = \frac{\sqrt{D} + P_0}{Q_0}$$

in einen Kettenbruch mit gewissen, noch näher zu bestimmenden Quotienten entwickelt.

Denn entwickelt man den rationalen Bruch $\frac{M_{n-1}}{N_{n-1}}$ in einen Kettenbruch $[a_0, a_1, a_2 \ldots a_{n-1}]$ und nimmt nun die entstehenden Quotienten der Reihe nach als willkürliche Quotienten der Entwickelung von $K = \frac{\sqrt{D} + P_0}{Q_0}$ an; so gilt für jeden Zeiger die Gl. (2) des §. 68. Offenbar sind aber die Zähler und Nenner des Näherungsbruches vom Zeiger $n - 1$ die Grössen M_{n-1}, N_{n-1}, für welche $\frac{M_{n-1}}{N_{n-1}} = [a_0, a_1 \ldots a_{n-1}]$ gebildet war. Es ist also die Eine Seite der Gl. (2) des §. 68 mit der betreffenden Seite der obigen Gl. (1) ganz identisch. Demnach müssen auch die anderen Seiten einander gleich sein, d. h. es muss der Werth der gegebenen Grösse $(-1)^n\, Q_n$ gleich der für den Zeiger n sich ergebenden Zahl aus der Reihe der Q, multiplizirt mit $(-1)^n$ sein.

Als Beispiel wollen wir statt Gl. (1) die folgende Gleichung

$$5x^2 + 6xy - 17y^2 = -50$$

nehmen. In Gestalt der Gl. (1) ist dieselbe

$$5x^2 - 2(-3)xy - 17y^2 = -50$$

Man hat hier $Q_0=5$, $P_0=-3$, $Q_{-1}=17$, also $D=(-3)^2+5.17=94$. Diese Gleichung ist erfüllt durch $x=9$, $y=7$. Entwickelt man den Bruch $\frac{x}{y}=\frac{9}{7}$ in einen Kettenbruch; so kommt $\frac{9}{7}=[1, 3, 2]$. Nimmt man diese Quotienten als Quotienten der Entwickelung von $K=\frac{\sqrt{94}-3}{5}$; so ergibt sich

$$x_0=\frac{\sqrt{94}-3}{5}=1+\frac{1}{x_1}$$

$$x_1=\frac{5}{\sqrt{94}-8}=\frac{\sqrt{94}+8}{6}=3+\frac{1}{x_2}$$

$$x_2=\frac{6}{\sqrt{94}-10}=\frac{\sqrt{94}+10}{-1}=2+\frac{1}{x_3}$$

$$x_3=\frac{-1}{\sqrt{94}+12}=\frac{\sqrt{94}-12}{50}$$

n	P_n	Q_n	$(-1)^n Q_n$	a_n	M_n	N_n
-2					0	1
-1		17	-17		1	0
0	-3	5	5	1	1	1
1	8	6	-6	3	4	3
2	10	-1	1	2	9	7
3	-12	50	-50			

Man sieht, dass hier in der That für den Zeiger $n-1=2$ die Grössen $M_2=9$, $N_2=7$ und für den Zeiger $n=3$ die Grösse $(-1)^3 Q_3=-50$ erscheint.

Wenn also der Werth auf der rechten Seite der gegebenen Gleichung (1) fähig ist, in irgend einer Entwickelung von $K=\frac{\sqrt{D}+P_0}{Q_0}$ unter den Grössen $(-1)^n Q_n$ zu erscheinen; so liefern Zähler und Nenner M_{n-1}, N_{n-1} des Näherungsbruches vom vorhergehenden Zeiger eine Auflösung jener Gleichung in relativ primen Zahlen.

Besitzt die rechte Seite jener Gleichung diese Fähigkeit nicht; so ist die Auflösung in relativ primen Zahlen **unmöglich**.

IV. Um nun jene rechte Seite der Gl. (1), welche wir jetzt mit q bezeichnen wollen, sodass

(4) $$q=(-1)^n Q_n \text{ also } Q_n=(-1)^n q=\pm q$$

ist, auf die zuletzt erwähnte Eigenschaft zu prüfen, und zugleich einen Weg zu finden, auf welchem man zu den von vorn herein unbekannten Quotienten $a_0, a_1 \ldots a_{n-1}$ und demnach zu der

gesuchten Auflösung $[a_0, a_1 \ldots a_{n-1}] = \frac{M_{n-1}}{N_{n-1}}$ gelangen kann, bemerken wir Folgendes.

Wenn q die fragliche Eigenschaft besitzt; so dass also eine Entwickelung von $K = \frac{\sqrt{D}+P_0}{Q_0}$ mit irgend welchen Quotienten auf ein Glied von der Form

(5) $$x_n = \frac{\sqrt{D}+P_n}{Q_n} = \frac{\sqrt{D}+P_n}{\pm q}$$

führen kann; so muss es nach §. 73 und 71 eine positive oder negative Zahl p geben, welche numerisch $\leqq \frac{1}{2} q$ und von solcher Beschaffenheit ist, dass die Entwickelung von

(6) $$K' = \frac{\sqrt{D}+p}{q}$$

mit grössten Subquotienten dieselbe Periode besitzt wie die Entwickelung von $K = \frac{\sqrt{D}+P_0}{Q_0}$.

V. Vor allen Dingen hat man also, da auch für die Grösse K' die Bedingung (2) in §. 59 erfüllt sein muss, diejenigen Werthe von p aufzusuchen, für welche

(7) $$\begin{cases} \frac{D-p^2}{q} = r \text{ eine ganze Zahl oder} \\ D-p^2 = rq \end{cases}$$

wird. Diese Untersuchung wird in den nächstfolgenden Paragraphen geführt werden.

VI. Hat man hierdurch einen zulässigen Werth für p gefunden, und sich überzeugt, dass die Entwickelung von K' dieselbe Periode besitzt, wie die von K; so kann man diese beiden Entwickelungen nach §. 73 kombiniren, also bewirken, dass $\pm q$ in der Reihe der Grössen $(-1)^n Q_n$ erscheint. Ergibt sich hierbei die letztere Grösse nicht bloss nach ihrem absoluten Werthe, was jedesmal der Fall sein wird; sondern auch nach ihrem Zeichen; so stellen M_{n-1}, N_{n-1} sofort eine gesuchte Auflösung dar.

Da sich zwei periodische Entwickelungen an unendlich vielen Stellen kombiniren lassen; so wird es im allgemeinen eine unendliche Menge von Auflösungen geben. Die Bequemlichkeit der Rechnung macht aber für die Ausführung dieser Kombinationen gewisse Vereinfachungen wünschenswerth, mit welchen wir uns in den §§. 82 ff. beschäftigen werden.

§. 75. Zahlenreihe, welche im Stande ist, die bei der Entwickelung der Quadratwurzel-Ausdrücke in Kettenbrüche vorkommenden Operationen zu ersetzen.

I. Wenn der Ausdruck $K = \frac{\sqrt{D}+P_0}{Q_0}$ zur Entwickelung in einen Kettenbruch gegeben ist; so sind die Grössen D, P_0, Q_0, $Q_{-1} = \frac{D - P_0^2}{Q_0}$ bekannt. Wird nun verlangt, dass die Entwickelung mit grössten Subquotienten vor sich gehe; so sind nicht allein die Grössen P_n, Q_n, sondern auch die Quotienten a_n gesucht. Verlangt man jedoch eine Entwickelung mit willkürlichen oder mit gegebenen Quotienten; so sind auch die Grössen a_n bekannt und nur noch P_n, Q_n gesucht.

Im ersteren Falle hat man zur Bestimmung der Grössen a_n, P_{n+1}, Q_{n+1} die drei Grundformeln

(1) $\frac{\sqrt{D}+P_n}{Q_n} = a_n + \frac{1}{x_{n+1}}$, worin x_{n+1} positiv und > 1,

(2) $P_{n+1} = a_n Q_n - P_n$ oder $P_n + P_{n+1} = a_n Q_n$

(3) $Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n}$ $Q_n Q_{n+1} = D - P_{n+1}^2$

im letzteren Falle dagegen kommen zur Bestimmung von P_{n+1}, Q_{n+1} nur die Formeln (2), (3) in Betracht.

II. Obgleich im Allgemeinen die Grössen P, Q, sowie die Quotienten, p o s i t i v und n e g a t i v sein können; so leuchtet doch ein, dass alle möglichen Werthe der Grösse $D - P^2$ erhalten werden, wenn man für P nach und nach bloss die p o s i t i v e n Werthe der aufsteigenden ganzen Zahlen 0, 1, 2, 3 . . . setzt, indem $(-P)^2 = (+P)^2$ ist.

Nach Gl. (3) ist klar, dass die Grössen Q F a k t o r e n der Glieder der Reihe

$$D,\ D-1,\ D-4,\ D-9\ \ldots\ D-p^2\ \ldots$$

welche Glieder wir kurz mit

$$J_0,\ J_1,\ J_2,\ J_3\ \ldots\ J_p\ \ldots$$

bezeichnen wollen, sind. Obgleich stets $J_{-p} = J_p$ ist; so hat doch das Z e i c h e n von p immer eine sehr wesentliche Bedeutung für die Entwickelung von K. Wir haben es also eigentlich mit einer D o p p e l r e i h e zu thun, in deren Mitte das Glied J_0 liegt.

Denken wir uns demnach für eine gegebene Determinante, z. B. für $D = 94$, diese Zahlenreihe J gebildet, fassen wir dann jedes Glied J_p, mit Ausnahme des Gliedes J_0, wie ein Doppelglied $J_{\pm 2}$ auf, von welchem der Eine Werth mit n e g a t i v e m Zeiger dem a b s t e i g e n d e n und der andere Werth mit p o s i t i v e m Zeiger dem a u f s t e i g e n d e n Schenkel einer nach beiden Seiten ins Unendliche sich fortsetzenden Reihe angehört;

so ergibt sich, wenn wir daneben auch die Primfactoren der einzelnen Glieder notiren,

	J_0	$94-0^2$	94	1.2.47
J_{-1}	J_1	$94-1^2$	93	1.3.31
J_{-2}	J_2	$94-2^2$	90	1.2.3.3.5
J_{-3}	J_3	$94-3^2$	85	1.5.17
J_{-4}	J_4	$94-4^2$	78	1.2.3.13
J_{-5}	J_5	$94-5^2$	69	1.3.23
J_{-6}	J_6	$94-6^2$	58	1.2.29
J_{-7}	J_7	$94-7^2$	45	1.3.3.5
J_{-8}	J_8	$94-8^2$	30	1.2.3.5
J_{-9}	J_9	$94-9^2$	13	1.13
α				α
J_{-10}	J_{10}	$94-10^2$	−6	−1.2.3
J_{-11}	J_{11}	$94-11^2$	−27	−1.3.3.3
J_{-12}	J_{12}	$94-12^2$	−50	−1.2.5.5
J_{-13}	J_{13}	$94-13^2$	−75	−1.3.5.5
J_{-14}	J_{14}	$94-14^2$	−102	−1.2.3.17
J_{-15}	J_{15}	$94-15^2$	−131	−1.131
J_{-16}	J_{16}	$94-16^2$	−162	−1.2.3.3.3.3
J_{-17}	J_{17}	$94-17^2$	−195	−1.3.5.13
J_{-18}	J_{18}	$94-18^2$	−230	−1.2.5.23
J_{-19}	J_{19}	$94-19^2$	−267	−1.3.89
J_{-20}	J_{20}	$94-20^2$	−306	−1.2.3.3.17

u. s. w.

Setzen wir die Determinante D wie früher $=a^2+b$, sodass a^2 die grösste unterhalb D liegende Quadratzahl ist; so werden die Glieder von $J_0=D$ bis $J_a=D-a^2=b$ positiv und bilden eine abnehmende Reihe; die jenseit J_a liegenden Glieder sind dagegen sämmtlich negativ und bilden numerisch eine zunehmende Reihe. Das zweideutige Glied null kann nirgends erscheinen. Durch die Linie αα haben wir die positiven Glieder von den negativen getrennt.

III. Wenn q ein Faktor irgend Einer der vorstehenden Zahlen $J_p=D-p^2$, also $D-p^2$ durch q theilbar oder

$$(4) \qquad \frac{D-p^2}{q}=r \text{ eine ganze Zahl oder } D-p^2=rq$$

ist, wobei p und q sowol positiv, wie negativ sein können; so kehrt jener Faktor q in allen Gliedern der obigen Reihe wieder, welche um q Glieder von einander abstehen. Diese spezielle Reihe der durch q theilbaren Zahlen setzt sich in einer leicht zu erkennenden Weise nach beiden Seiten ins Unendliche fort, und ausgehend von irgend Einem dieser Glieder, kann man alle übrigen durch einfache Abzählung finden. So hat man z. B. für $q=5$, wenn man von dem Gliede $J_7=45=9.5$ ausgeht,

$$\begin{array}{lllllll} \ldots J_{-13} & J_{-8} & J_{-3} & J_{2} & J_{7} & J_{12} & J_{17}\ldots \\ =\ldots -75 & 30 & 85 & 90 & 45 & -50 & -195\ldots \\ =\ldots -15.5 & 6.5 & 17.5 & 18.5 & 9.5 & -10.5 & -39.5\ldots \end{array}$$

IV. Kehrt man in einer solchen Reihe J_p das Zeichen von p um; so ergibt sich für J_{-p} eine zweite Reihe ebenfalls durch q theilbarer Zahlen, in welcher die Werthe der einzelnen Glieder mit den vorstehenden genau übereinstimmen. Diese zweite Reihe, welche im letzteren Beispiele beim Fortschritte von unten nach oben

$$\ldots J_{-17} \quad J_{-12} \quad J_{-7} \quad J_{-2} \quad J_{3} \quad J_{8} \quad J_{13}\ldots$$

sein würde, wollen wir die konjugirte der ersteren nennen.

V. Allgemein hat man, wenn w eine beliebige positive oder negative ganze Zahl bezeichnet,

$$(5)\qquad J_{\pm p + wq} = D - (\pm p + wq)^2 = D - p^2 \mp 2wpq - w^2 q^2 = (r \mp 2wq - w^2 q)\,q$$

sodass der andere Faktor von q in diesem Gliede $= r \mp 2wq - w^2 q$ ist. Setzt man

$$(6)\qquad -p + wq \text{ oder } wq - p = p' \text{ und}$$

$$(7)\qquad r + 2wq - w^2 q = r'$$

so erkennt man sofort die Identität der in §. 61 vorkommenden Grössen und Formeln mit den gegenwärtigen. Wir wollen dieselben zur besseren Übersicht einander gegenüber stellen.

$$(8)\quad \left\{ \begin{array}{ll} D & D \\ P_n & p \\ Q_n & q \\ a_n & w \\ Q_{n-1} = \dfrac{D - P_n^2}{Q_n} & r = \dfrac{D - p^2}{q} \\ Q_{n-1} Q_n = D - P_n^2 & rq = D - p^2 \\ P_{n+1} = a_n Q_n - P_n & p' = wq - p \\ Q_{n+1} = Q_{n-1} + 2a_n P_n - a_n^2 Q_n & r' = r + 2wp - w^2 q \\ Q_{n+1} Q_n = D - P_{n+1}^2 & r' q = D - p'^2 \\ x_n = \dfrac{\sqrt{D} + P_n}{Q_n} = a_n + \dfrac{1}{x_{n+1}} & x_n = \dfrac{\sqrt{D} + p}{q} = w + \dfrac{1}{x_{n+1}} \\ x_{n+1} = \dfrac{\sqrt{D} + P_{n+1}}{Q_{n+1}} & x_{n+1} = \dfrac{\sqrt{D} + p'}{r'} \end{array} \right.$$

VI. Hiernach ist es nun leicht, sich der obigen Zahlenreihe J zu bedienen, um die in der Entwickelung von $x_n = \dfrac{\sqrt{D} + P_n}{Q_n}$ auftretenden Grössen $P_{n+1}, P_{n+2}, P_{n+3}\ldots$ und $Q_{n+1}, Q_{n+2}, Q_{n+3}\ldots$ durch einfache Abzählungen und Divisionen darzustellen, wenn für die Quotienten $a_n, a_{n+1}, a_{n+2}\ldots$ beliebige Grössen gegeben sind. Hierbei fassen wir die Reihe J immer als eine nach beiden Seiten ins Unendliche sich erstreckende oder als Doppelreihe auf, indem wir die Zählungsrichtung von J_- ge-

gen J_+ die **positive** oder **vorwärts gehende** und die von J_+ gegen J_- die **negative** oder **rückwärts gehende** nennen. Man operirt folgendermaassen:

Da $P_n = p$, $Q_n = q$, $a_n = w$ bekannt (positiv oder negativ) sind; so geht man, um zunächst $P_{n+1} = p' = -p + wq$ zu bilden, in das Glied J_{-p} ein, dessen Zeiger $-p$ den **entgegengesetzten** Werth von p hat. Haben w und q **gleiche Zeichen**, ist also wq **positiv**; so zählt man von jenem Gliede **vorwärts** $w$mal q Glieder ab: haben dagegen w und q **ungleiche Zeichen**, ist also wq **negativ**; so zählt man von jenem Gliede **rückwärts** dieselbe Anzahl von Gliedern ab. Hierdurch gelangt man in das Glied $J_{-p+wq} = J_{p'} = D - p'^2 = r'q$, also zu dem Werthe $P_{n+1} = p' = -p + wq$. Dividirt man dieses Glied durch $Q_n = q$; so ist der Quotient $\frac{r'q}{q} = r' = Q_{n+1}$.

Nachdem man so P_{n+1} und Q_{n+1} gefunden hat, ergibt sich nach demselben Prinzipe mit Hülfe des ferneren Quotienten a_{n+1} der Werth von P_{n+2} und Q_{n+2}, indem man von dem Gliede $J_{-p'}$ ausgeht, u. s. f.

Auf diesem Wege erhält man z. B. aus $K = \frac{\sqrt{94} + 3}{5}$ für die willkürlichen Quotienten 2, -1, 1, 0, -1, 3 folgende Werthe.

n	P_n	Q_n	a_n
-1		17	
0	3	5	2
1	7	9	-1
2	-16	-18	1
3	-2	-5	0
4	2	-18	-1
5	16	9	3
6	11	-3	

VII. Will man aber die Entwickelung von K mit **grössten Subquotienten** darstellen; so sind die Quotienten $a_n = w$ nicht mehr von vorn herein gegeben oder willkürlich, sondern an die Bedingung geknüpft, dass wenn der genaue Werth von

$$x_n = \frac{\sqrt{D} + P_n}{Q_n}$$

zwischen den

positiven Zahlen c und $c+1$ liegt, $a_n = w = c$ sei

[illegible] » 0 » 1 » » » $= 0$ »

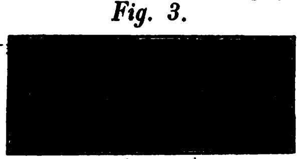
[illegible]ven » $-(c+1)$ » $-c$ » » » $= -(c+1)$ »

[illegible] Zahl $a_n = w$ lässt sich nun unter diesen Bedingungen se[illegible]ht aus der obigen Zahlenreihe J, sowol ihrem absolute[illegible]ge, wie ihrem Zeichen nach, durch Abzählung von dem Gl[illegible]$_{-p}$ aus bestimmen, wodurch man dann auch das folgende Gl[illegible] $= r'q$, mithin $P_{n+1} = p'$ und $Q_{n+1} = \frac{r'q}{q} = r'$ erhält.

Man hat hierbei nach folgenden leicht zu konstatirenden Regeln zu verfahren, welche wir zu grösserer Deutlichkeit graphisch darstellen wollen. Bei dieser graphischen Darstellung bezeichnet der Pfeil die Richtung, in welcher man vom Gliede J_{-p} aus bis zum Gliede $J_{p'}$ fortzuzählen hat, indem das Gefieder der Stelle des Zeigers $-p$ und die Spitze der Stelle des Zeigers p' entspricht. Wenn die Pfeilspitze in Beziehung zu der die positiven und negativen Zahlen J trennenden Linie $\alpha\alpha$ Eine der beiden in Fig. 2 dargestellten Lagen hat, so soll damit angedeutet werden, dass man sich der Linie $\alpha\alpha$ von der betreffenden Seite her soviel, als es nur möglich ist, nähere, also bis zu der nächsten auf jener Seite vor der Linie $\alpha\alpha$ liegenden durch q theilbaren Zahl $J_{p'}$ schreiten muss. Wenn dagegen die Pfeilspitze Eine der beiden in Fig. 3 dargestellten Lagen hat; so soll damit angedeutet werden, dass man die Linie $\alpha\alpha$ nach der betreffenden Seite hin eben überschreiten, also bis zu der nächsten jenseit der Linie $\alpha\alpha$ liegenden durch q theilbaren Zahl $J_{p'}$ schreiten muss. Bei dieser Bewegung vom Gliede J_{-p} aus zählt man immer Komplexe von je q Gliedern ab. Wäre unter den vorstehenden Bedingungen gar kein Fortschritt möglich; so entspricht Dies dem Falle $a_n = 0$.

Fig. 2.

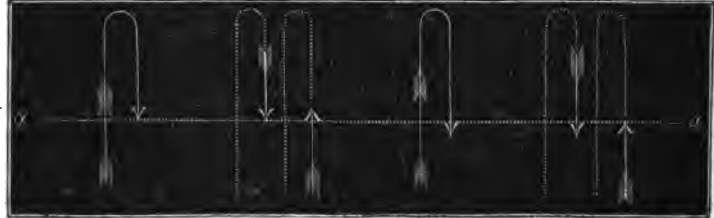
Fig. 3.



Ob a_n positiv oder negativ sei, entscheidet sich unter gleichzeitiger Berücksichtigung des Zeichens von q nach der desfallsigen früheren Erläuterung. Man erkennt aber leicht, dass a_n stets positiv ist, wenn man nach Fig. 1 diesseit der Linie $\alpha\alpha$ bleibt, dagegen stets negativ, wenn man nach Fig. 2 die Linie $\alpha\alpha$ überschreitet, gleichviel in welcher Richtung die Bewegung erfolgt.

Fig. 4.

	I.	II.	III.	IV.
	$\frac{\sqrt{D}+p}{q}$	$\frac{\sqrt{D}-p}{q}$	$\frac{\sqrt{D}+p}{-q}$	$\frac{\sqrt{D}-p}{-q}$
$a_n =$	0, 1, 2 . . .	0, 1, 2 . . . | −1, −2, −3 . . .	−1, −2, −3 . . .	−1, −2, −3 . . . | 0, 1, 2 . . .



Hiernach wird die Fig. 4, welche die Regeln für die verschiedenen möglichen Fälle darstellt, verständlich sein. In den Überschriften müssen unter p und q absolute Werthe gedacht werden, sodass $-p$ und $-q$ negativ sind. Man überzeugt sich, dass der zweideutige Fall, wofür $p=0=\pm 0$ ist, durchaus mit keiner Unsicherheit behaftet ist.

Als Erläuterung zu vorstehender Figur mögen folgende spezielle Fälle dienen.

ad I. $\frac{\sqrt{94}+5}{23} = 0+\frac{1}{x}, \frac{\sqrt{94}+5}{3} = 4+\frac{1}{x},$

$\frac{\sqrt{94}+11}{27} = 0+\frac{1}{x}, \frac{\sqrt{94}+13}{15} = 1+\frac{1}{x}$

ad II. $\frac{\sqrt{94}-8}{15} = 0+\frac{1}{x}, \frac{\sqrt{94}-4}{2} = 2+\frac{1}{x},$

$\frac{\sqrt{94}-14}{2} = -3+\frac{1}{x}$

ad III. $\frac{\sqrt{94}+8}{-15} = -2+\frac{1}{x}, \frac{\sqrt{94}+11}{-27} = -1+\frac{1}{x}$

ad IV. $\frac{\sqrt{94}-4}{-2} = -3+\frac{1}{x}, \frac{\sqrt{94}-14}{-17} = 0+\frac{1}{x},$

$\frac{\sqrt{94}-14}{-2} = 2+\frac{1}{x}$

Da in der Periode von K jede Grösse $P<\sqrt{D}$ oder $\leqq a$ ist; so folgt, dass sich in dieser Periode die vorstehende Bewegung auf die oberhalb der Linie $\alpha\alpha$ liegenden positiven Glieder von J_0 bis J_s beschränken wird.

Man erkennt leicht, dass wenn p und p_1 zwei beliebige Glieder Ein und derselben durch q theilbaren Zahlenreihe sind, sodass man also $p_1=p+wq$ hat, die Entwickelungen von $\frac{\sqrt{D}+p}{q}$ und von $\frac{\sqrt{D}+p_1}{q}=\frac{\sqrt{D}+p}{q}+w$ mit grössten Subquotienten schon bei der nächsten Entwickelungsstufe genau zu denselben Grössen führt (§. 72).

§. 76. *Erste Methode der Aufsuchung aller Reihen der durch q theilbaren Zahlen J durch Bestimmung des Gliedes mit kleinstem Zeiger in jeder Reihe.*

Es kommt uns jetzt darauf an, alle verschiedenen Reihen der durch q theilbaren Zahlen zu finden. Da die Zeiger der Glieder einer jeden solchen Reihe um q Einheiten von einander abstehen; so genügt es, von jeder verschiedenen Reihe ein einziges Glied zu bestimmen. Hierzu wollen wir gegenwärtig das Glied J_p mit dem kleinsten Zeiger p ausersehen.

Von je zwei konjugirten Reihen brauchen wir offenbar nur Eine zu bestimmen, indem die Umkehrung der Zeichen der Zeiger dieser Reihe sofort die andere ergibt. Im Allgemeinen sind die beiden konjugirten Reihen verschieden. Für den Fall, dass sie gleich sind, dass also ihre Glieder in der Gesammtreihe J aufeinander fallen, wollen wir die Eine Reihe, welche alsdann statt der beiden konjugirten in Betracht kommt, eine symmetrische nennen.

Da, wie schon erwähnt, die Differenz zwischen zwei benachbarten Zeigern einer jeden gesuchten Zahlenreihe $=q$ ist; so muss von jeder möglichen Reihe dieser Art jedenfalls Ein Glied, aber auch nur Ein Glied, wenn q paar ist, unter den Zahlen

$$\text{von } J_{-\frac{q}{2}} \text{ bis } J_{\frac{q}{2}}$$

und wenn q unpaar ist, unter den Zahlen

$$\text{von } J_{-\left(\frac{q}{2}-\frac{1}{2}\right)} \text{ bis } J_{\frac{q}{2}-\frac{1}{2}}$$

vorkommen. Betrachten wir also nur positive Zeiger p; so muss von zwei konjugirten Reihen die Eine ein Glied besitzen, dessen Zeiger nicht grösser als $\frac{q}{2}$ ist.

Man bildet also die Zahlen

$$D-0^2, D-1^2, D-2^2, D-3^2 \ldots \begin{cases} D-\left(\frac{q}{2}\right)^2 & \text{wenn } q \text{ paar ist} \\ D-\left(\frac{q-1}{2}\right)^2 & \text{wenn } q \text{ unpaar ist} \end{cases}$$

und untersucht, welche derselben durch q theilbar sind.

Ist keine durch q theilbar; so gibt es überhaupt keine durch q theilbare Zahl von der Form $J_p=D-p^2$.

Jede Zahl $J_p=D-p^2$ dagegen, welche sich unter den genannten durch q theilbar erweis't, gehört einer besonderen gesuchten Reihe an. $J_{-p}=D-(-p)^2$ ist dann ein Glied der konjugirten Reihe.

Wenn für eine solche Reihe $p=0$ ist; so ist die konjugirte Reihe mit derselben identisch. Man hat es also dann mit einer symmetrischen Reihe zu thun.

Dasselbe findet statt, wenn sich $p=\frac{q}{2}$ findet, was jedoch nur dann möglich ist, wenn q paar ist.

In anderen als diesen beiden Fällen können offenbar symmetrische Reihen nicht auftreten.

Es sei z. B. $D=94$, $q=30$; alsdann sind die Zahlen von $J_0=94$ bis $J_{\frac{q}{2}}=J_{15}=94-15^2=-131$ zu bilden. Dieselben sind schon in §. 75 angegeben. Man findet, dass darunter zwei

Zahlen, nämlich $J_2 = 90$ und $J_8 = 30$ durch $q = 30$ theilbar sind. Demnach hat man unter Berücksichtigung der konjugirten Reihen folgende vier verschiedene durch 30 theilbare Zahlenreihen.

$$\begin{array}{ccccc} \ldots J_{-58} & J_{-28} & J_2 & J_{32} & J_{62} \ldots \\ \ldots J_{-62} & J_{-32} & J_{-2} & J_{28} & J_{58} \ldots \\ \ldots J_{-52} & J_{-22} & J_8 & J_{38} & J_{68} \ldots \\ \ldots J_{-68} & J_{-38} & J_{-8} & J_{22} & J_{52} \ldots \end{array}$$

§. 77. ***Zweite und meistens einfachere Methode der Aufsuchung aller Reihen der durch* q *theilbaren Zahlen* J *durch Bestimmung des zweiten Faktors* r.**

Aus der Gleichung $D - p^2 = rq$ folgt

(1) $$D - rq = p^2$$

Es muss also die Grösse $D - qr$ ein vollkommenes Quadrat und zwar von dem Zeiger p eines Gliedes der zu untersuchenden Reihe sein. Wir fassen das schon im vorhergehenden Paragraphen betrachtete Glied dieser Reihe ins Auge, für welches der Zeiger p den kleinsten Werth hat, und bestimmen die Gränzen, innerhalb welcher die Zahl r liegen muss. Man braucht alsdann nur die diesen Gränzen entsprechenden Vielfachen der Grösse q von D zu subtrahiren und nachzusehen, welche Reste ein vollkommenes Quadrat p^2 liefern.

Es ist offenbar nur nöthig die Annahme zu machen, dass q positiv sei. Denn wäre q negativ; so brauchte man die durch gegenwärtige Methode für positive q sich ergebenden Werthe von r nur mit entgegengesetztem Zeichen zu nehmen.

Da nach dem vorhergehenden Paragraphen der Zeiger p des von zwei konjugirten Reihen zunächst an der Zahl J_0 liegenden Gliedes, jenachdem q paar oder unpaar ist, zwischen 0 und $\frac{q}{2}$ oder zwischen 0 und $\frac{q-1}{2}$, mithin der Werth qr dieses Gliedes zwischen D und $D - \left(\frac{q}{2}\right)^2$ oder zwischen D und $D - \left(\frac{q-1}{2}\right)^2$ liegt; so ist klar, dass der Werth $r = \frac{D - p^2}{q}$ des zweiten Faktors jenes Gliedes zwischen $\frac{D}{q}$ und $\frac{D - \left(\frac{q}{2}\right)^2}{q}$ oder zwischen $\frac{D}{q}$ und $\frac{D - \left(\frac{q-1}{2}\right)^2}{q}$ liegen muss. Die erste Gränze von r ist positiv, die zweite kann jedoch sowol positiv, wie negativ, wie null sein, jenachdem $D >, <, = \left(\frac{q}{2}\right)^2$ oder

$\left(\frac{q-1}{2}\right)^2$ ist. Bezeichnet also

r_0 den grössten Subquotienten von $\frac{D}{q}$ und

r_1 den kleinsten Superquotienten von $\frac{D-\left(\frac{q}{2}\right)^2}{q}$ oder

$\frac{D-\left(\frac{q-1}{2}\right)^2}{q}$, jenachdem q paar oder unpaar ist, wobei r_0 nicht kleiner als null, r_1 aber sehr wohl negativ werden kann; so hat man in die Formel (2) für r nach und nach die Werthe

$$r_0 \quad r_0-1 \quad r_0-2 \quad r_0-3 \quad \ldots \quad r_1$$

zu substituiren. Die Differenz zwischen r_0 und r_1 kann niemals den Werth der Differenz $\frac{D}{q}-\frac{D-\left(\frac{q}{2}\right)^2}{q}=\frac{q}{4}$ übersteigen, sodass im Allgemeinen Eine Substitution mehr zu machen sein wird, als ganze Zahlen unterhalb des Werthes $\frac{q}{4}$ liegen. Da nun aber die eben genannten Substitutionen zu folgenden Werthen

$$(D-r_0q) \quad (D-r_0q)+q \quad (D-r_0q)+2q \quad (D-r_0q)+3q\ldots$$
$$(D-r_0q)+(r_0-r_1)q$$

führen; so hat man ganz einfach die Grösse $D-r_0q$ zu bilden und dieselbe als erstes Glied einer Reihe zu nehmen, wovon jedes folgende um q Einheiten grösser ist als das vorhergehende. So oft man hierdurch auf ein vollkommenes Quadrat p^2 stösst, hat man den Zeiger p einer durch q theilbaren Zahl J gefunden, welche immer einer neuen Reihe angehört. Ist für ein solches Glied $(D-r_0q)+mq$ d. i. $D-(r_0-m)\,q=p^2$; so hat man für den zweiten Faktor $r=r_0-m$.

Das gegenwärtige Verfahren erfordert, wenn wir kurz mit $\frac{q}{4}$ die ganze Zahl r_0-r_1 andeuten, nur die $\left(\frac{q}{4}\right)$malige Addition einer konstanten Grösse q und Vergleichung der sich ergebenden Zahlen mit einer Tafel der Quadratzahlen, um diejenigen zu markiren, welche vollkommene Quadrate sind. Das Verfahren des vorhergehenden Paragraphen dagegen erforderte die doppelte Anzahl viel umständlicherer Operationen, nämlich die $\left(\frac{q}{2}\right)$malige Subtraktion verschiedener Quadrate und Untersuchung, welche der entstehenden Zahlen durch q

theilbar seien, welches Letztere noch ebenso viel Divisionen oder die Zuhülfenahme einer Faktorentafel nöthig macht.

Beispiel 1. Es sei $D=94$, $q=102$, also q paar und $\frac{q}{2}=51$. Jetzt ist $\frac{D}{q}=\frac{94}{102}$, $\frac{D-\left(\frac{q}{2}\right)^2}{q}=\frac{94-51^2}{102}=-24\frac{97}{102}$, also $r_0=0$, $r_1=-24$, $r_0-r_1=24$ und zuvörderst $D-r_0q=94$. Dies gibt folgende Rechnung

r	$\frac{D-rq}{102=q}$
$r_0=0$	94
-1	$196=14^2$
-2	298
-3	$400=20^2$
-4	502
-5	604
-6	706
-7	808
-8	910
-9	1012
-10	1114
-11	1216
-12	1318
-13	1420
-14	1522
-15	1624
-16	1726
-17	1828
-18	1930
-19	2032
-20	2134
-21	2236
-22	2338
-23	2440
$r_1=-24$	2542

Demnach hat man in diesem Falle die beiden Reihen resp. für $p=14$ und $p=20$

.	.
.	.
.	.
$J_{-292}=-835.102$	$J_{-286}=-801.102$
$J_{-190}=-353.102$	$J_{-184}=-331.102$
$J_{-88}=-75.102$	$J_{-82}=-65.102$
$J_{14}=-1.102$	$J_{20}=-3.102$
$J_{116}=-131.102$	$J_{122}=-145.102$
$J_{208}=-465.102$	$J_{224}=-491.102$
.	.
.	.
.	.

und ausserdem die konjugirte von jeder dieser Reihen, für welche nur die Zeiger die entgegengesetzten Zeichen annehmen, für welche also Ein Glied resp. den Zeiger $p=-14$ und $p=-20$ hat.

Beispiel 2. Es sei $D=94$, $q=23$, also q unpaar und $\frac{q-1}{2}=11$.

Jetzt ist $\frac{D}{q}=\frac{94}{23}=4\frac{2}{23}$, $\frac{D-\left(\frac{q-1}{2}\right)^2}{q}=\frac{94-11^2}{23}=-1\frac{4}{23}$, also $r_0=4$, $r_1=-1$, $r_0-r_1=5$ und zuvörderst $D-r_0q=2$. Dies gibt folgende Rechnung

r	$D-rq$
	$23=q$
$r_0=4$	2
3	$25=5^2$
2	48
1	71
0	94
$r_1=-1$	117

Demnach hat man in diesem Falle für $p=5$ die Reihe

$$J_{-41}=-69.23$$
$$J_{-18}=-10.23$$
$$J_5=3.23$$
$$J_{28}=-30.23$$

und ausserdem die konjugirte Reihe.

Beispiel 3. Es sei $D=94$, $q=13$, also q unpaar und $\frac{q-1}{2}=6$.

Jetzt ist $\frac{D}{q}=\frac{94}{13}=7\frac{3}{13}$, $\frac{D-\left(\frac{q-1}{2}\right)^2}{q}=\frac{94-6^2}{13}=4\frac{6}{13}$, also $r_0=7$, $r_1=5$, $r_0-r_1=2$ und zuvörderst $D-r_0q=3$. Dies gibt folgende Rechnung

r	$D-rq$
	$13=q$
$r_0=7$	3
6	$16=4^2$
$r_1=5$	29

Demnach hat man in diesem Falle für $p=4$ die Reihe

$$J_{-9}=1.13$$
$$J_4=6.13$$
$$J_{17}=-10.13$$

und dazu die konjugirte Reihe.

Beispiel 4. Es sei $D=94$, $q=6$, also q paar und $\frac{q}{2}=3$.

Jetzt ist $\frac{D}{q}=\frac{94}{6}=15\frac{4}{6}$, $\frac{D-\left(\frac{q}{2}\right)^2}{q}=\frac{94-3^2}{6}=14\frac{1}{6}$, also $r_0=15$, $r_1=15$, $r_0-r_1=0$. Ist mithin nicht schon $D-r_0q=4$ ein vollkommenes Quadrat; so gibt es eine gesuchte Reihe überall nicht. In der That ist aber dieser Werth $4=2^2$ ein Quadrat; man hat also für $p=2$ die Reihe

$$\begin{matrix} \ldots J_{-10} & J_{-4} & J_2 & J_8 & J_{14}\ldots \\ =\ldots-1.6 & 13.6 & 15.6 & 5.6 & -17.6\ldots \end{matrix}$$

und daneben die konjugirte Reihe.

§. 78. *Abkürzung der vorstehenden Rechnung für sehr grosse Werthe von q.*

I. Wenn die Zahl q sehr gross ist, wird es erwünscht sein, die vorstehende Rechenarbeit, obgleich dieselbe nur in Additionen besteht, soviel als möglich abzukürzen, indem man diejenigen zwischen den Gränzen r_0 und r_1 für r liegenden Zahlen von der Form $D-rq$, welche unmöglich vollkommene Quadrate werden können, von der Berechnung ausschliesst.

Zu diesem Ende erwäge man, dass eine Quadratzahl nur mit Einer der sechs Ziffern 0, 1, 4, 5, 6, 9 schliessen kann, dass also jede Zahl, welche mit Einer der vier Ziffern 2, 3, 7, 8 schliesst, unmöglich ein Quadrat sein kann. Die aus $D - rq$ hervorgehenden Zahlen der letzteren Art lassen sich aber leicht von der Berechnung ausschliessen, wenn man statt der im vorigen Paragraphen bezeichneten Einen Tabelle deren zehn anlegt, in deren jeder r nicht um 1, sondern um 10 variirt. In jeder dieser zehn Tabellen werden alle Zahlen mit derselben Ziffer schliessen; man unterdrückt daher gleich von vorn herein diejenigen Tabellen, welche mit Einer der Ziffern 2, 3, 7, 8 schliessen würden.

Wäre z. B. $D = 11$, $q = 327$, also q unpaar und $\frac{q-1}{2} = 163$, ferner $\frac{D}{q} = \frac{11}{327}$, $\frac{D - \left(\frac{q-1}{2}\right)^2}{q} = \frac{11 - 163^2}{327} = -81\frac{71}{327}$, mithin $r_0 = 0$, $r_1 = -81$, $r_0 - r_1 = 81$ und $D - r_0 q = 11$; so stellen wir zur besseren Übersicht erst den Anfang der Einen Tabelle aus dem vorhergehenden Paragraphen für die zehn ersten Werthe von r dar. Dies gibt

r	$D - rq$
	$327 = q$
$r_0 =$ 0	11
-1	338
-2	665
-3	992
-4	1319
-5	1646
-6	1973
-7	2300
-8	2627
-9	2954

Hieraus erkennt man, dass die vier mit $r = -1, -3, -6, -8$ anfangenden Tabellen auszuschliessen sind, indem die Zahlen $D - rq$ derselben resp. mit 8, 2, 3, 7 schliessen, folglich durchaus keine Quadrate liefern würden.

Demnach hat man es nur mit sechs Tabellen zu thun, welche resp. mit $r = 0, -2, -4, -5, -7, -9$ anfangen. Dieselben sind, indem man beachtet, dass jetzt statt q immer das 10fache davon, also $10q = 3270$ zu addiren ist,

r	$D-rq$	r	$D-rq$	r	$D-rq$	r	$D-rq$	r	$D-rq$	r	$D-rq$
	3270		3270		3270		3270		3270		3270
0	11	-2	665	-4	1319	-5	1646	-7	2300	-9	2954
-10	3281	-12	3935	-14	4589	-15	4916	-17	5570	-19	6224
-20	6551	-22	7205	-24	7859	-25	8186	-27	8840	-29	9494
-30	9821	-32	10475	-34	11129	-35	11456	-37	12110	-39	12764
-40	13091	-42	13745	-44	14399	-45	14726	-47	15380	-49	16034
-50	16361	-52	17015	-54	17669	-55	17996	-57	18650	-59	19304
-60	19631	-62	20285	-64	20939	-65	21266	-67	21920	-69	22574
-70	22901	-72	23555	-74	24209	-75	24536	-77	25190	-79	35844
-80	26171										

Da hierunter kein Quadrat vorkommt; so kann es keine durch $q = 327$ theilbare Zahl von der Form $D - p^2 = 11 - p^2$ geben.

II. Die vorstehende Abkürzung genügt bis zu dem Werthe von etwa $\frac{q}{4} = 100$ oder $q = 400$. Ist q noch bedeutend grösser bis $\frac{q}{4} = 1000$ also $q = 4000$; so kann man, nachdem man in jeder der zuletzt beschriebenen Tabellen 10 Glieder berechnet hat, noch eine grössere Menge von Zahlen durch die Betrachtung unterdrücken, dass die zwei letzten Ziffern eines Quadrats nur die folgenden sein können.

00	01	04	25	16	09
	21	24		36	29
	41	44		56	49
	61	64		76	69
	81	84		96	89

Dies sind von 100 möglichen nur 22 zulässige Kombinationen, also etwa der 5te Theil.

Berücksichtigt man ferner, dass wenn man in $D - rq$ die Grösse r um 100 variiren lässt, die zwei letzten Ziffern der entstehenden Zahlen immer dieselben sein werden; so kann man in den zuletzt erwähnten Tabellen alle diejenigen Zahlen unterdrücken, deren letzte zwei Ziffern der vorstehenden Bedingung nicht entsprechen. Aus den übrig bleibenden bildet man die Anfangsglieder von ebenso viel neuen Tabellen, in welchen r um 100 variirt und demnach immer der Werth $100\,q$ zu addiren ist.

Wollte man hiernach in dem letzteren Beispiele die Zahlenbildung über $r = -100$ fortsetzen (was hier nur den Zweck der Erläuterung unseres Rechnungsverfahrens hat); so würde man aus der ersten Tabelle nur die Werthe $D - 10\,q = 3281$, $D - 30\,q = 9821$, $D - 50\,q = 16361$, $D - 70\,q = 22901$, $D - 90\,q = 29441$ beizubehalten haben, was zunächst fünf neue Tabellen ergibt, wovon die erste

r	$D - rq$
	$32700 = 100\,q$
-10	3281
-110	35981
-210	38681
-310	71381

u. s. w.

ist. Aus der zweiten obigen Tabelle würde nur die einzige Zahl $D - 82\,q = 26825$ beizubehalten sein, welche die neue Tabelle

r	$D-rq$
	$32700=100q$
-82	26825
-182	59525
-282	92225
-382	124925
	u. s. w.

ergibt, u. s. w.

III. Käme $\frac{q}{4}$ an 10000 oder q an 40000; so könnte man nach dem vorstehenden Prinzipe fortfahren, nachdem man in jeder der zuletzt berechneten Tabellen 10 Glieder berechnet hätte, diejenigen zu unterdrücken, welche unter Berücksichtigung der drei letzten Ziffern zu keinen Quadraten führen können. Bei den neu zu bildenden Tabellen variirt alsdann r um 1000 und es ist immer 1000 q zu addiren; u. s. f. Die drei Ziffern, welche den Schluss einer Quadratzahl bilden können, sind in folgender Tabelle zusammengestellt

dritte Ziffer von hinten	die letzten zwei Ziffern	dritte Ziffer von hinten	die letzten zwei Ziffern
0, 1, 4, 5, 6, 9	00	0, 2, 6	25
0, 2, 4, 6, 8	01	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	16
1, 3, 5, 7, 9	21	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	36
0, 2, 4, 6, 8	41	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	56
1, 3, 5, 7, 9	61	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	76
0, 2, 4, 6, 8	81	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	96
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	04	0, 2, 4, 6, 8	09
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	24	1, 3, 5, 7, 9	29
0. 1, 2, 3, 4, 5, 6, 7, 8, 9	44	0, 2, 4, 6, 8	49
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	64	1, 3, 5, 7, 9	69
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	84	0, 2, 4, 6, 8	89

Dies sind 159 zulässige von 1000 möglichen Formen, also nur der 6te bis 7te Theil.

§. 79. *Vereinfachung für den Fall, dass Faktoren der Zahl* q *bekannt sind.*

I. Eine wesentliche Erleichterung der nach §. 77 anzustellenden Ermittelung stellt sich heraus, sobald von der Zahl q relativ prime Faktoren bekannt sind. Angenommen, es sei $q=q'q''q'''$ ... und keine zwei der Faktoren q', q'', q''' besitzen ein gemeinschaftliches Maass. Zuvörderst ist klar, dass die durch q theilbare Zahl von der Form $D-p^2$ durch jeden einzelnen der Faktoren q', q'', q''' ... theilbar sein muss. Man kann also damit beginnen, alle möglichen Reihen der Zahlen J aufzusuchen, welche resp. durch q', q'', q''' ... theilbar sind. Findet sich schon hierbei, dass es für Einen

dieser Faktoren eine gesuchte Reihe nicht gibt; so ist die ganze Aufgabe unmöglich.

Findet man aber für jeden Faktor Eine oder mehrere Reihen; so hat man von jeder dieser Reihen die Werthe der nicht über $\frac{q}{2}$, resp. nicht über $\frac{q-1}{2}$ liegenden Zeiger zu bilden und nachzusehen, welche Zeiger von gleichem Werthe gleichzeitig in einer Reihe für q', in einer Reihe für q'', in einer Reihe für q''' u. s. w. vorkommen. Gibt es solche übereinstimmende Zeiger nicht; so ist der Fall unmöglich. Gibt es deren aber; so bezeichnen dieselben ebensoviel Reihen, deren Glieder durch das Produkt $q'q''q''' \ldots = q$ theilbar sind.

So hätte man z. B. die ganze Rechnung des §. 78 für den Fall $D=11$, $q=327$ vermeiden können, wenn man beachtete, dass $327 = 3.109$ ist, dass also $11 - p^2$ sowol durch 3, als auch durch 109 theilbar sein muss. Nun findet man leicht, dass es keine durch 3 theilbare Zahl von dieser Form geben kann. Demnach ist die ganze Aufgabe unmöglich.

Wäre $D=94$, $q=90$ gegeben; so könnte man $90 = 9.10$ setzen. Für $q'=9$ findet sich folgende Zahlenreihe, in welcher statt der negativen Zeiger nur deren absolute Werthe angedeutet sind, und welche überhaupt nur so weit ausgedehnt ist, dass die Zeiger nicht grösser als $\frac{q}{2} = 45$ sind.

$$J_{43} \quad J_{34} \quad J_{25} \quad J_{16} \quad J_{7} \quad J_{2} \quad J_{11} \quad J_{20} \quad J_{29} \quad J_{38}$$

Für $q''=10$ findet sich folgende ebensoweit ausgedehnte Zahlenreihe

$$J_{38} \quad J_{28} \quad J_{18} \quad J_{8} \quad J_{2} \quad J_{12} \quad J_{22} \quad J_{32} \quad J_{42}$$

In diesen beiden Reihen kommen gleichzeitig die Glieder J_2 und J_{38} vor. Man hat also folgende zwei durch $q=90$ theilbare Zahlenreihen

$$\ldots J_{-178} \quad J_{-88} \quad J_{2} \quad J_{92} \quad J_{182} \ldots$$
$$\ldots J_{-142} \quad J_{-52} \quad J_{38} \quad J_{128} \quad J_{218} \ldots$$

und ausserdem die konjugirten derselben.

II. Wenn man es unter Umständen für bequemer hält, kann man auch, nachdem man Eine Reihe für q' ermittelt und bis zu den angegebenen Gränzen ausgedehnt hat, nachsehen, welche Glieder davon durch q'' theilbar sind. Die letzteren werden dann offenbar auch durch $q'q''$ theilbar sein.

So findet man im letzten Beispiele, dass aus der Reihe für $q'=9$ die beiden Glieder J_2 und J_{38} durch $q'=10$ theilbar sind.

III. Es wird noch bemerkt, dass wenn für jede von zwei relativ primen Zahlen q' und q'' eine Reihe der fraglichen Art besteht, nothwendig auch für das Produkt $q'q''=q$ eine solche bestehen muss. Denn ist p' ein Zeiger der ersten Reihe und

p'' ein solcher der zweiten Reihe; so kann man, weil q' und q'' relativ prim sind, stets zwei ganze Zahlen x und y so bestimmen, dass $p'+q'x=p''+q''y$ oder $q'x-q''y=p''-p'$ ist (§. 28). Es gibt also in der ersten Reihe einen Zeiger $p'+xq'$, welcher einem Zeiger $p''+yq''$ in der zweiten Reihe gleich ist, und welcher demnach einem durch $q'q''=q$ theilbaren Gliede angehört.

Der letztere Satz gilt offenbar auch von mehr als zwei Faktoren q', q'', q''' ... von denen keine zwei ein gemeinschaftliches Maass besitzen, also von den Primfaktoren, resp. deren Potenzen, in welche sich die Zahl q zerlegen lässt.

IV. Im Vorstehenden ist vorausgesetzt, dass keine zwei der Faktoren q', q'', q''' ... von q ein gemeinschaftliches Maass besitzen. Wäre diese Bedingung nicht erfüllt, und wollte man nicht durch Absonderung aller gemeinschaftlichen Maasse die Grösse q in lauter solche Faktoren zerlegen, von denen je zwei relativ prim wären; so müsste man, nachdem durch das obige Verfahren die durch q', q'', q''' ... einzeln theilbaren Zahlen J von gleichen Zeigern p ermittelt sind, ausdrücklich prüfen, ob diese Zahlen auch durch das Produkt $q=q'q''q'''$ ... theilbar sind, was nicht immer der Fall sein wird.

Nähme man z. B. im obigen speziellen Falle, wo $D=94$ ist, $q=90=3.30$ an; so würden die durch $q'=3$ theilbaren Zahlen die Reihe

$$J_{44} \ldots J_8 \quad J_5 \quad J_2 \quad J_1 \quad J_4 \quad J_7 \quad J_{10} \ldots J_{43}$$

und die durch $q''=30$ theilbaren Zahlen die beiden Reihen

$$J_{28} \quad J_2 \quad J_{32}$$
$$J_{22} \quad J_8 \quad J_{38}$$

bilden. Man findet, dass die 6 Zeiger 2, 8, 22, 28, 32, 38 der letzten beiden Reihen sämmtlich unter den Zeigern der ersten Reihe vorkommen. Dies würde, wenn $q'=3$ und $q''=30$ relativ prim wären, 6 verschiedene Reihen der durch 90 theilbaren Zahlen liefern. Es haben jedoch q' und q'' das gemeinschaftliche Maass 3, und wenn man demnach untersucht, welche der letzteren 6 Zahlen durch 90 theilbar sind; so findet man nur J_2 und J_{38}, also nur die beiden schon früher ermittelten Reihen.

§. 80. Fall, wo q eine Primzahl ist.

Wenn q eine Primzahl ist; so kann es nur eine einzige Reihe der durch q theilbaren Zahlen und die konjugirte Reihe davon geben, wenn überhaupt eine durch q theilbare Zahl J möglich ist. In diesem Falle würde man also die zur Ermittelung eines Gliedes dieser Reihe dienende Rechnung sofort abbrechen, nachdem man Einen Werth von p gefunden hat.

Der Beweis der vorstehenden Behauptung ist einfach. Wenn eine Zahl $J_p = D - p^2 = rq$ ist und nun eine andere Zahl $J_{p+x} = D - (p+x)^2 = D - p^2 - 2px - x^2$ ebenfalls ein Vielfaches von q, also $= Rq$ sein soll; so muss man wegen $D - p^2 = rq$

$$rq - 2px - x^2 = Rq \text{ also}$$

$$r - \frac{(2p+x)x}{q} = R$$

haben. Hiernach muss offenbar $\frac{(2p+x)x}{q}$ eine ganze Zahl sein. Das Letztere ist, wenn q eine Primzahl ist, nur auf zweierlei Weise möglich. Entweder ist q in x enthalten, also $x = wq$, folglich die Zahl $D - (p+x)^2 = D - (p+wq)^2$ nur ein anderes Glied der Reihe, in welcher auch die Zahl $D - p^2$ liegt; oder es ist q in $2p+x$ enthalten, also $2p+x = wq$, folglich $x = -2p+wq$ und die Zahl $D - (p+x)^2 = D - (-p+wq)^2$ ein Glied der zur vorstehenden konjugirten Reihe.

Demnach können nur die zusammengesetzten Zahlenwerthe von q zu mehr als Einer selbstständigen Reihe führen (wozu noch die konjugirte Reihe kommt).

§. 81. *Spezielle Fälle.*

In manchen Fällen kann man ohne weitere Rechnung wenigstens Eine der gesuchten durch q theilbaren Zahlenreihen darstellen. Zu den wichtigsten Fällen dieser Art gehören die folgenden.

I. Für $q = 1$ ist die Gesammtreihe der Zahlen J in §. 75 die stets mögliche und zugleich symmetrische Reihe der gesuchten Zahlen. Die Zeigerfolge ist also $\ldots -3, -2, -1, 0, 1, 2, 3 \ldots$

II. Für $q = 2$ ist, weil die Zahlen J abwechselnd paar und unpaar sind, stets Eine, aber auch nur Eine gesuchte Reihe möglich, welche auch immer symmetrisch ist. Wenn D paar ist; so hat man für die Zeigerfolge $\ldots -4, -2, 0, 2, 4 \ldots$ und wenn D unpaar ist, $\ldots -3, -1, 1, 3 \ldots$

III. Für $q = 3$ geht, wenn D die Form $3n$ hat, stets eine Reihe durch das Glied J_0, und wenn D die Form $3n+1$ hat, also $D - 1$ durch 3 theilbar ist, durch das Glied J_1. Wenn aber D die Form $3n+2$ hat; so ist keine Reihe möglich, weil hier $q = 3$ unpaar, $\frac{q-1}{2} = 1$ und weder J_0 noch J_1 durch q theilbar ist.

IV. Für $q = 4$ geht, wenn D die Form $4n$ hat, stets eine Reihe durch J_0, und wenn D die Form $4n+1$ hat, also $D - 1$ durch 4 theilbar ist, durch J_1. Wenn aber D die Form $4n+2$ oder $4n+3$ hat, ist keine Reihe möglich, da hier, wo $q = 4$ paar

und $\frac{q}{2}=2$ ist, weder $J_0=D$, noch $J_1=D-1$, noch $J_2=D-4$ durch 4 theilbar ist.

V. Für $q=D$ oder $=$ einem Faktor von D gibt es ausser anderen möglichen Reihen stets eine symmetrische mit der Zeigerfolge $\ldots -2q,\ -q,\ 0,\ q,\ 2q \ldots$

VI. Für $q=D-1$ oder $=$ einem Faktor von $D-1$ gibt es ausser anderen möglichen Reihen stets die mit der Zeigerfolge $\ldots -(2q-1),\ -(q-1),\ 1,\ (q+1),\ (2q+1) \ldots$ und die konjugirte Reihe davon.

VII. Wenn q aus zwei Faktoren besteht, welche in zwei benachbarten Zahlen J_p und J_{p+1} der Gesammtreihe J enthalten sind (wobei es nicht nöthig ist, dass diese Faktoren relativ prim seien); so gibt es stets eine Reihe der durch q theilbaren Zahlen. Denn es ist das Produkt aus den beiden Zahlen J_p und J_{p+1} identisch

$$(D-p^2)\,[D-(p+1)^2]=-\left\{ D-[D-p(p+1)]^2\right\}$$

Demnach ist das Produkt der beiden Zahlen J_p und J_{p+1} das Entgegengesetzte einer Zahl J vom Zeiger $D-p(p+1)$. Es kommen also alle Faktoren der beiden Zahlen J_p und J_{p+1}, folglich auch die Zahl q in Einer der Zahlen J vor.

Aus Vorstehendem folgt, wenn man beachtet, dass D und $D-1$ zwei benachbarte Zahlen J_0 und J_1 sind, dass für $q=D\,(D-1)$ oder $=$ jedem beliebigen Faktor von $D(D-1)$ stets eine gesuchte Reihe besteht. Der absolute Werth des gesammten Produktes $D(D-1)$ wiederholt sich in dem Gliede vom Zeiger D, indem man hat

$$J_D=-J_0\,J_1=D-D^2$$

In dem letzteren Satze sind die beiden vorhergehenden ad V. und VI. mit eingeschlossen.

VIII. Zu dem obigen Satze V. bemerken wir noch, dass wenn q ein Faktor von D oder $=D$ ist, und q keinen quadratischen Faktor enthält, nur die einzige Reihe mit der Zeigerfolge $\ldots -2q,\ -q,\ 0,\ q,\ 2q \ldots$ möglich ist.

Denn nach der Voraussetzung hat man $D=rq$, also $\frac{D}{q}=r$. Für irgend eine durch q theilbare Zahl J hat man $D-p^2=Rq$ also $r-\frac{p^2}{q}=R$; es muss also für eine solche Zahl $\frac{p^2}{q}$ eine ganze Zahl sein. Wenn nun q keinen quadratischen Faktor besitzt; so muss q in p enthalten, also p ein Vielfaches von q sein. Unter solchen Umständen liegt aber p in der Zeigerfolge der vorgedachten Reihe.

IX. Nach diesen Sätzen erkennt man z. B., dass für $D = 94 = 2.47$, wofür $D - 1 = 93 = 3.31$ ist, die Werthe

$q = 1$ 2 3 2.3 31 47 2.31 3.31 2.47 3.47 2.3.31 2.3.47 31.47 2.31.47 3.31.47 2.3.31.47
$= 1$ 2 3 6 31 47 62 93 94 141 186 282 1457 2914 4371 8742

jedenfalls mögliche Reihen ergeben müssen.

Weitere Untersuchungen über diesen Gegenstand verschieben wir auf §. 155 ff.

§. 82. *Rekursionsformel für die Näherungswerthe Ein und desselben Kettenbruchs, welche um die Länge der Periode von einander abstehen.*

In §. 74 ist angedeutet, wie wichtig für die unbestimmten Gleichungen vom zweiten Grade es ist, möglichst bequeme Methoden zur Berechnung der sukzessiven Näherungsbrüche zu besitzen, welche sich durch die Kombination zweier unendlicher Kettenbrüche mit gleichen Perioden ergeben.

Der einfachste hierher gehörige Fall ist der, wo die Näherungswerthe Ein und desselben Kettenbruchs, welche um die Periodenlänge von einander abstehen, zu berechnen sind.

Der gegebene Kettenbruch sei

(1) $$K = [a_0, a_1, a_2 \ldots]$$

Die Periode umfasse r Glieder, der Zeiger $n+1$ liege irgend wo in einer Periode und es komme darauf an, die Zähler und Nenner der Näherungsbrüche $K_n, K_{n+r}, K_{n+2r} \ldots$ zu bestimmen. Zu diesem Ende bilden wir zuvörderst aus den Quotienten der mit dem Zeiger $n+1$ beginnenden Periode den endlichen Kettenbruch

(2) $$\mathfrak{K} = [a_{n+1}, a_{n+2}, a_{n+3} \ldots a_{n+r}] = [\mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2 \ldots \mathfrak{a}_{r-1}]$$

Der gesammte oder letzte Näherungswerth von $\mathfrak{K}$ ist $\mathfrak{K}_{r-1} = \frac{\mathfrak{M}_{r-1}}{\mathfrak{N}_{r-1}}$; der vorletzte Näherungswerth davon ist $\mathfrak{K}_{r-2} = \frac{\mathfrak{M}_{r-2}}{\mathfrak{N}_{r-2}}$. Setzen wir die Zahlen $\mathfrak{M}_{r-1}, \mathfrak{N}_{r-1}, \mathfrak{M}_{r-2}, \mathfrak{N}_{r-2}$ als berechnet voraus; so haben wir nach §. 15

(3) $$M_{n+r} = \mathfrak{M}_{r-1} M_n + \mathfrak{N}_{r-1} M_{n-1}$$ und ähnlich ist

(4) $$M_{n+r-1} = \mathfrak{M}_{r-2} M_n + \mathfrak{N}_{r-2} M_{n-1}$$

Wie nun die Grösse M_{n+r} aus M_n und M_{n-1} durch die Elemente $a_{n+1}, a_{n+2} \ldots a_{n+r}$ entstanden ist, ebenso entsteht wegen der periodischen Wiederkehr dieser Elemente die Grösse M_{n+2r} aus M_{n+r} und M_{n+r-1}. Man hat also

(5) $$M_{n+2r} = \mathfrak{M}_{r-1} M_{n+r} + \mathfrak{N}_{r-1} M_{n+r-1}$$

Eliminirt man zwischen den beiden Gleichungen (3), (4) die Grösse M_{n-1}; so kommt, wenn man die Grundformel $\mathfrak{M}_{r-2} \mathfrak{N}_{r-1} - \mathfrak{M}_{r-1} \mathfrak{N}_{r-2} = (-1)^{r-1}$ §. 4 betrachtet,

(6) $$\mathfrak{N}_{r-1}\, M_{n+r-1} = \mathfrak{N}_{r-2}\, M_{n+r} + (-1)^{r-1}\, M_n$$

Substituirt man diesen Werth in Gl. (5); so kommt

(7) $M_{n+2r} = (\mathfrak{M}_{r-1} + \mathfrak{N}_{r-2})\, M_{n+r} + (-1)^{r-1}\, M_n$ und ähnlich ist

(8) $M_{n+2r-1} = (\mathfrak{M}_{r-1} + \mathfrak{N}_{r-2})\, M_{n+r-1} + (-1)^{r-1}\, M_{n-1}$

In den Formeln (3) bis (8) kann offenbar auch das Zeichen N an die Stelle von M gesetzt werden, um statt der Zähler die Nenner der betreffenden Näherungsbrüche zu ergeben.

Setzen wir die aus dem Kettenbruche $\mathfrak{K}$, Gl. (2) leicht zu bestimmende Grösse

(9) $$\mathfrak{M}_{r-1} + \mathfrak{N}_{r-2} = h$$

und nehmen wir die beiden Näherungsbrüche $K_n = \frac{M_n}{N_n}$ und $K_{n+r} = \frac{M_{n+r}}{N_{n+r}}$ als bereits berechnet an; so haben wir für die Zähler und Nenner der Näherungsbrüche von den Zeigern $n+2r$, $n+3r$, $n+4r\ldots$ wegen der vorstehenden Beziehungen folgende Rekursionsformel

$$\begin{array}{ll} M_{n+2r} = h\, M_{n+r} + (-1)^{r-1}\, M_n & N_{n+2r} = h\, N_{n+r} + (-1)^{r-1}\, N_n \\ M_{n+3r} = h\, M_{n+2r} + (-1)^{r-1}\, M_{n+r} & N_{n+3r} = h\, N_{n+2r} + (-1)^{r-1}\, N_{n+r} \\ M_{n+4r} = h\, M_{n+3r} + (-1)^{r-1}\, M_{n+2r} & N_{n+4r} = h\, N_{n+3r} + (-1)^{r-1}\, N_{n+2r} \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \end{array}$$

(10) $$\begin{cases} M_{n+pr} = h\; M_{n+(p-1)r} + (-1)^{r-1}\; M_{n+(p-2)r} \\ N_{n+pr} = h\; N_{n+(p-1)r} + (-1)^{r-1}\; N_{n+(p-2)r} \end{cases}$$

Ist nun die Gliederzahl r der Periode unpaar, mithin $r-1$ paar und $(-1)^{r-1} = +1$; so erzeugen sich die Werthe der um die Periodenlänge voneinander abstehenden Näherungsbrüche K_{n+2r}, $K_{n+3r}\ldots$ ebenso wie die benachbarten Näherungswerthe eines nach dem Additionsprinzipe gebildeten Kettenbruchs, dessen Quotienten sämmtlich $= h$ sind, indem man für dessen Näherungswerthe vom Zeiger 0 und 1 resp. die Brüche $\frac{M_n}{N_n}$ und $\frac{M_{n+r}}{N_{n+r}}$ annimmt, nach folgendem bekannten Schema

0		M_n	N_n
1		M_{n+r}	N_{n+r}
2	h	M_{n+2r}	N_{n+2r}
3	h	M_{n+3r}	N_{n+3r}
4	h	M_{n+4r}	N_{n+4r}
.	.	.	.
.	.	.	.
.	.	.	.

Beispiel 1. Es sei $K = [1, 3, 2, \underbrace{5, 1, 1}, \underbrace{5, 1, 1}, \ldots]$ gegeben, um die Näherungswerthe K_2, K_5, K_8, $K_{11}\ldots$ zu bilden. Man hat $n=2$, $r=3$, $r-1=2$, $(-1)^{r-1} = +1$ und zur Bestimmung von K_2, K_5 sowie von $h = \mathfrak{M}_2 + \mathfrak{N}_1$ hat man

$K=[1, 3, 2, 5, 1, 1 \ldots]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	3	4	3
2	2	9	7
3	5	49	38
4	1	58	45
5	1	107	83

$\mathfrak{K}=[5, 1, 1]$

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	5	5	1
1	1	6	1
$r-1=2$	1	11	2

$\mathfrak{M}_{r-1}=\mathfrak{M}_2=11$

$M_n \;=M_2=9 \qquad N_n \;=N_2=7 \qquad \mathfrak{N}_{r-2} = \mathfrak{N}_1 \;=1$

$M_{n+r}=M_5=107 \qquad N_{n+r}=N_5=83 \qquad h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}=12$

Wir haben also hier statt Gl. (10) die Formel

$$M_{3p+2}=12\,M_{3p-1}+M_{3p-4} \qquad N_{3p+2}=12\,N_{3p-1}+N_{3p-4}$$

und demnach folgende Rechnung

n	h	M_n	N_n
2		9	7
5		107	83
8	12	1293	1003
11	12	15623	12119
14	12	188769	146431
17	12	2280851	1769291

u. s. w.

Ist dagegen die Gliederzahl r der Periode paar, mithin $r-1$ unpaar und $(-1)^{r-1}=-1$; so erzeugen sich die fraglichen Näherungsbrüche ebenso wie die benachbarten Näherungswerthe eines nach dem Subtraktionsprinzipe gebildeten Kettenbruchs mit lauter gleichen Quotienten h (§. 23). Man hat jetzt die vorhergehende Grösse wie M_n von dem $h$fachen der folgenden Grösse M_{n+r} zu subtrahiren, statt dass man vorhin addirte, um M_{n+2r} zu erhalten.

Beispiel 2. Es sei $K=[0, 3, \underbrace{4, 1, 1, 2}, \underbrace{4, 1, 1, 2} \ldots]$ gegeben, um die Näherungswerthe K_1, K_5, K_9, $K_{13} \ldots$ zu bestimmen. Hier ist $n=1$, $r=4$, $r-1=3$, $(-1)^{r-1}=-1$ und zur Bestimmung von K_1, K_5, sowie von $h=\mathfrak{M}_3+\mathfrak{N}_2$ hat man

$K=[0, 3, 4, 1, 1, 2 \ldots]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	3	1	3
2	4	4	13
3	1	5	16
4	1	9	29
5	2	23	74

$\mathfrak{K}=[4, 1, 1, 2]$

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	4	4	1
1	1	5	1
2	1	9	2
$r-1=3$	2	23	5

$\mathfrak{M}_{r-1}=\mathfrak{M}_3=23$

$M_n \;=M_1=1 \qquad N_n \;=N_1=3 \qquad \mathfrak{N}_{r-2} = \mathfrak{N}_2=2$

$M_{n+r}=M_5=23 \qquad N_{n+r}=N_5=74 \qquad h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}=25$

Hier gilt also für Gl. (10) die Formel

$$M_{4p+1} = 25\, M_{4p-3} - M_{4p-7} \qquad N_{4p+1} = 25\, N_{4p-3} - N_{4p-7}$$

welche zu folgender Rechnung führt

n	k	M_n	N_n
1		1	3
5		23	74
9	25	574	1847
13	25	14327	46101
17	25	357601	1150678

u. s. w.

§. 83. *Rekursionsformel für die Werthe von Kettenbrüchen, welche entstehen, wenn zwischen zwei bestimmten Quotienten eines gegebenen Kettenbruchs Ein und dieselbe Periode mehrmals eingeschaltet wird.*

Der in der Überschrift dieses Paragraphen bezeichnete Fall, welcher den des vorhergehenden Paragraphen als Spezialität mit einschliesst, hat für die unbestimmten Gleichungen vom zweiten Grade eine noch grössere Wichtigkeit. Derselbe erfordert die Bestimmung folgender Werthe

$$(1) \qquad \overset{0}{K} = \frac{\overset{0}{M}}{\overset{0}{N}} = [a_0,\ a_1 \ldots\ a_n,\ b_1,\ b_2 \ldots\ b_q]$$

$$(2) \qquad \overset{1}{K} = \frac{\overset{1}{M}}{\overset{1}{N}} = [a_0,\ a_1 \ldots\ a_{n+r},\ b_1,\ b_2 \ldots\ b_q]$$

$$(3) \qquad \overset{2}{K} = \frac{\overset{2}{M}}{\overset{2}{N}} = [a_0,\ a_1 \ldots\ a_{n+2r},\ b_1,\ b_2 \ldots\ b_q]$$

u. s. w. Man kann sich die Entstehung derselben auch so vorstellen, dass ein unendlicher periodischer Kettenbruch

$$(4) \qquad K = [a_0,\ a_1, \ldots\ldots]$$

in dessen Periode von r Gliedern der Zeiger $n+1$ liegt, erst vor der ersten, dann vor der zweiten, dann vor der dritten Periode u. s. w. abgebrochen werde, indem man hinter der Stelle des Abbruches immer die Quotienten b_1, $b_2 \ldots\ b_q$ anhängt. Für das immer Einmal mehr eingeschaltete periodische Stück wollen wir, wie im vorhergehenden Paragraphen

$$(5) \qquad \mathfrak{K} = \frac{\mathfrak{M}_{r-1}}{\mathfrak{N}_{r-1}} = [a_{n+1},\ a_{n+2} \ldots\ a_{n+r}] = [\mathfrak{a}_0,\ \mathfrak{a}_1 \ldots\ \mathfrak{a}_{r-1}]$$

und für das am Ende angehängte Stück

$$(6) \qquad K' = \frac{M'_{q-1}}{N'_{q-1}} = [b_1,\ b_2 \ldots\ b_q] = [a'_0,\ a'_1 \ldots\ a'_{q-1}]$$

schreiben.

Vor allen Dingen machen wir zur Vermeidung von Missverständnissen darauf aufmerksam, dass die Näherungswerthe (1), (2), (3) ... mit darüber geschriebenen Zeigern keineswegs Ein und demselben Kettenbruche angehören.

Wir nehmen nun an, die zwei Näherungsbrüche $\overset{0}{K}$ und $\overset{1}{K}$ aus (1) und (2) seien bereits berechnet, und es komme darauf an, die folgenden $\overset{2}{K}$, $\overset{3}{K}$... mit Hülfe jener zu bestimmen.

Beziehen wir zu diesem Ende die Grössen K, M, N mit darunter gesetzten Zeigern $n-1$, n, $n+r-1$, $n+r$, $n+2r-1$, $n+2r$ auf den Kettenbruch (4); so haben wir zunächst nach den Prinzipien des vorhergehenden Paragraphen, aus welchen die dortige Gl. (3) geflossen ist,

(7) $$\overset{0}{M} = M'_{q-1}\, M_n + N'_{q-1}\, M_{n-1}$$

(8) $$\overset{1}{M} = M'_{q-1}\, M_{n+r} + N'_{q-1}\, M_{n+r-1}$$

(9) $$\overset{2}{M} = M'_{q-1}\, M_{n+2r} + N'_{q-1}\, M_{n+2r-1}$$

Ausserdem aber haben wir nach denselben Prinzipien, wenn wir auch hier

(10) $$h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2}$$

setzen,

(11) $$M_{n+2r} = h\, M_{n+r} + (-1)^{r-1}\, M_n$$

(12) $$M_{n+2r-1} = h\, M_{n+r-1} + (-1)^{r-1}\, M_{n-1}$$

Substituirt man die Werthe (11), (12) in (9); so kommt

$$\overset{2}{M} = h(M'_{q-1}\, M_{n+r} + N'_{q-1}\, M_{n+r-1}) + (-1)^{r-1}\, (M'_{q-1}\, M_n + N'_{q-1}\, M_{n-1})$$

d. i. wegen (8) und (7)

(13) $$\overset{2}{M} = h\, \overset{1}{M} + (-1)^{r-1}\, \overset{0}{M}$$

und in ähnlicher Weise findet sich

$$\overset{3}{M} = h\, \overset{2}{M} + (-1)^{r-1}\, \overset{1}{M}$$

$$\overset{4}{M} = h\, \overset{3}{M} + (-1)^{r-1}\, \overset{2}{M}$$

$$\vdots$$

(14) $$\overset{n}{M} = h\, \overset{n-1}{M} + (-1)^{r-1}\, \overset{n-2}{M}$$

In diesen Rekursionsformeln kann man auch zur Bestimmung der Nenner N das Zeichen N statt M schreiben.

Diese Formeln haben eine ähnliche Bildung wie die ad (10) im vorhergehenden Paragraphen, und entsprechen demnach, jenachdem die eingeschaltete Periode eine unpaare oder paare Gliederzahl r besitzt, oder jenachdem $(-1)^{r-1} = +1$ oder -1 ist, einer Erzeugung nach dem Additions- oder Subtraktionsprinzipe.

Beispiel 1. Es sei $K=[0, \underbrace{2, 1, 3}, \underbrace{2, 1, 3} \ldots]$ und indem erst hinter $n=0$, dann hinter $n+r=3$, dann hinter $n+2r=6$ u. s. w. abgebrochen wird, soll immer $K'=[5, 4]$ angehängt werden, sodass nach und nach die Werthe von

$$\overset{0}{K}=[0, 5, 4],\ \overset{1}{K}=[0, 2, 1, 3, 5, 4],\ \overset{2}{K}=[0, 2, 1, 3, 2, 1, 3, 5, 4]$$

u. s. w. zu bilden sind.

Hier ist $n=0$, $q=2$, $r=3$, $r-1=2$, $(-1)^{r-1}=+1$, und zur Bestimmung von $\overset{0}{K}$, $\overset{1}{K}$, sowie von $h=\mathfrak{M}_2+\mathfrak{N}_1$ hat man

$\overset{0}{K}=[0, 5, 4]$

n	a_n	M_n	N_n
−2		0	1
−1		1	0
0	0	0	1
1	5	1	5
2	4	4	21

$\overset{0}{M}=4$

$\overset{0}{N}=21$

$\overset{1}{K}=[0, 2, 1, 3, 5, 4]$

n	a_n	M_n	N_n
−2		0	1
−1		1	0
0	0	0	1
1	2	1	2
2	1	1	3
3	3	4	11
4	5	21	58
5	4	88	243

$\overset{1}{M}=88$

$\overset{1}{N}=243$

$\mathfrak{K}_{r-1}=[2, 1, 3]$

$\mathfrak{n}$	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
−2		0	1
−1		1	0
0	2	2	1
1	1	3	1
$r-1=2$	3	11	4

$\mathfrak{M}_{r-1}=\mathfrak{M}_2=11$

$\mathfrak{N}_{r-2}=\mathfrak{N}_1=1$

$h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}=12$

Hier hat man also für Gl. (14) die Formeln

$$\overset{n}{M}=12\overset{n-1}{M}+\overset{n-2}{M} \qquad \overset{n}{N}=12\overset{n-1}{N}+\overset{n-2}{N}$$

und Dies gibt folgende Rechnung

n	h	$\overset{n}{M}$	$\overset{n}{N}$
0		4	21
1		88	243
2	12	1060	2937
3	12	12808	35487
4	12	154756	428781

u. s. w.

Beispiel 2. Es sei $K=[0, \underbrace{2, 1, 3, 1}, \underbrace{2, 1, 3, 1} \ldots]$ und indem erst hinter $n=0$, dann hinter $n+r=4$, dann hinter $n+2r=8$ u. s. w. abgebrochen wird, werde wie vorhin $K'=[5, 4]$ angehängt.

Hier ist $n=0$, $q=2$, $r=4$, $r-1=3$, $(-1)^{r-1}=-1$ und zur Bestimmung von $\overset{0}{K}$, $\overset{1}{K}$, sowie von $h=\mathfrak{M}_3+\mathfrak{N}_2$ hat man

$\overset{0}{K} = [0, 5, 4]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	5	1	5
2	4	4	21

$\overset{0}{M} = 4$

$\overset{0}{N} = 21$

$\overset{1}{K} = [0, 2, 1, 3, 1, 5, 4]$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	2	1	2
2	1	1	3
3	3	4	11
4	1	5	14
5	5	29	81
6	4	121	338

$\overset{1}{M} = 121$

$\overset{1}{N} = 338$

$\mathfrak{K}_{r-1} = [2, 1, 3, 1]$

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	2	2	1
1	1	3	1
2	3	11	4
$r-1=3$	1	14	5

$\mathfrak{M}_{r-1} = \mathfrak{M}_3 = 14$

$\mathfrak{N}_{r-2} = \mathfrak{N}_2 = 4$

$h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2} = 18$

Dies gibt statt Gl. (14) die Formeln

$$\overset{n}{M} = 18\overset{n-1}{M} - \overset{n-2}{M} \qquad \overset{n}{N} = 18\overset{n-1}{N} - \overset{n-2}{N}$$

und demnach folgende Rechnung

n	h	$\overset{n}{M}$	$\overset{n}{N}$
0		4	21
1		121	338
2	18	2174	6063
3	18	39011	128796
4	18	663187	2312265

u. s. w.

§. 84. Rekursionsformel für sämmtliche Kombinationen zweier periodischer Kettenbrüche.

I. Die beiden zu kombinirenden Kettenbrüche seien

(1) $K = [a_0, a_1 \ldots a_m, c_1, c_2 \ldots c_r, c_1, c_2 \ldots c_r, c_1, c_2 \ldots]$

(2) $K' = [b_0, b_1 \ldots b_n, c_1, c_2 \ldots c_r, c_1, c_2 \ldots c_r, c_1, c_2 \ldots]$

sodass $c_1, c_2 \ldots c_r$ die gemeinschaftliche r-gliedrige Periode ist.

Man kann hier jeden Werth von $K(m)$, $(m+r)$, $(m+2r)\ldots$ mit jedem Werthe von $K'(n)$, $(n+r)$, $(n+2r)\ldots$ kombiniren. Dies gibt nach §. 73 zwei besondere Systeme. Die Kombinationen des Einen Systems sind dargestellt durch

(3) $K(m)\ komb.\ K'(n) = [a_0, a_1 \ldots a_m, 0, -b_n, -b_{n-1} \ldots -b_1]$

(4) $K(m+r)\ komb.\ K'(n) = [a_0, a_1 \ldots a_m, c_1, c_1 \ldots c_r, 0, -b_n, -b_{n-1} \ldots -b_1]$

(5) $K(m+2r)\ komb.\ K'(n) = [a_0, a_1 \ldots a_m, c_1, c_2 \ldots c_r, c_1, c_2 \ldots c_r, 0, -b_n, -b_{n-1} \ldots -b_1]$

u. s. w. Die Kombinationen des anderen Systems sind dargestellt durch

(6) $K(m)\ komb.\ K'(n) = [a_0, a_1 \ldots a_m, 0, -b_n, -b_{n-1} \ldots -b_1]$

(7) $K(m)\ komb.\ K'(n+r) = [a_0, a_1 \ldots a_m, 0, -c_r, -c_{r-1} \ldots -c_1, -b_n, -b_{n-1} \ldots -b_1]$

(8) $K(m)$ *komb.* $K'(n+2r) = [a_0, a_1 \ldots a_m, 0, -c_r, -c_{r-1} \ldots -c_1, -c_r, -c_{r-1} \ldots -c_1, -b_n, -b_{n-1} \ldots -b_1]$

u. s. w.

II. Eine jede folgende Kombination in jedem System unterscheidet sich von der vorhergehenden nur dadurch, dass Eine und dieselbe Periode, nämlich im ersten Systeme die Periode $c_1, c_2 \ldots c_r$ und im zweiten Systeme die Periode $-c_r, -c_{r-1} \ldots -c_1$ Einmal mehr eingeschaltet ist. Wir wollen jetzt zeigen, dass beide Systeme nach Ein und derselben Rekursionsformel gebildet werden können.

Zu diesem Ende bezeichnen wir die Gesammtwerthe der Kombinationen (3), (4), (5 ... mit $\overset{0}{K}, \overset{1}{K}, \overset{2}{K} \ldots$ und die der Kombinationen (6), (7), (8) mit $\overset{0}{K}, \overset{-1}{K}, \overset{-2}{K} \ldots$, nehmen $\overset{0}{K}, \overset{1}{K}$ als bekannt und $\overset{2}{K}, \overset{3}{K} \ldots$ sowie $\overset{-1}{K}, \overset{-2}{K} \ldots$ als gesucht an. Zuvörderst hat man nach dem vorhergehenden Paragraphen, wenn

(9) $h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2}$ aus $\mathfrak{K}_{r-1} = [c_1, c_2 \ldots c_r]$

bestimmt ist,

(10) $$\overset{2}{M} = h\overset{1}{M} + (-1)^{r-1}\overset{0}{M}$$

Ferner hat man, wenn

(11) $h' = \mathfrak{M}'_{r-1} + \mathfrak{N}'_{r-2}$ aus $\mathfrak{K}'_{r-1} = [-c_r, -c_{r-1} \ldots -c_1]$

bestimmt ist,

(12) $$\overset{-2}{M} = h'\overset{-1}{M} + (-1)^{r-1}\overset{0}{M}$$

Nach §. 13 ist aber für die Zähler der letzten Näherungsbrüche von $\mathfrak{K}$ und $\mathfrak{K}'$, indem man die entgegengesetzten Zeichen der Quotienten von $\mathfrak{K}'$ mit beachtet, $\mathfrak{M}'_{r-1} = (-1)^r \mathfrak{M}_{r-1}$ und für die Nenner der vorletzten Näherungsbrüche $\mathfrak{N}'_{r-2} = (-1)^{r-2}\mathfrak{N}_{r-2} = (-1)^r \mathfrak{N}_{r-2}$ demnach ist

(13) $h' = (-1)^r h$ folglich

(14) $$\overset{-2}{M} = (-1)^r h\overset{-1}{M} + (-1)^{r-1}\overset{0}{M}$$

Hiernach ist, wenn man $(-1)^{r-1}\overset{0}{M}$ auf Einer Seite stehen lässt, und mit dem Koeffizienten $(-1)^{r-1}$ multiplizirt,

(15) $\overset{0}{M} = h\overset{-1}{M} + (-1)^{r-1}\overset{-2}{M}$ und ebenso erhält man

$$\overset{-1}{M} = h\overset{-2}{M} + (-1)^{r-1}\overset{-3}{M}$$

$$\overset{-2}{M} = h\overset{-3}{M} + (-1)^{r-1}\overset{-4}{M}$$

u. s. w. Diese Formeln sind nach demselben Gesetze gebildet, wie die Gleichung (10) für $\overset{2}{M}$ und die Grössen $\overset{3}{M}, \overset{4}{M} \ldots$ Man sieht, dass in der Mitte zwischen diesen beiden Systemen noch die Existenz der Formel

$$\overset{1}{M} = h\overset{0}{M} + (-1)^{r-1}\overset{-1}{M}$$

nachgewiesen werden müsste, um beide Systeme als ein einziges, gesetzmässig zusammenhängendes erscheinen zu lassen.

III. Um diese Beziehung zwischen den Grössen $\overset{1}{M}$ und $\overset{-1}{M}$, welches die Zähler der Werthe der Kettenbrüche (4) und (7) sind, darzustellen; so beachte man, dass diese beiden Kettenbrüche denselben Anfang $[a_0, a_1 \ldots a_m]$, also zuvörderst die Werthe M_{m-1}, M_m gemein haben. Setzen wir nun die Bildung für $\overset{1}{M}$ mittelst der Quotienten aus (4) fort, indem wir dabei von den Werthen M_{m-1} und M_m ausgehen und die aus den folgenden Quotienten entstehenden Faktoren nach dem Prinzipe des §. 12 bezeichnen; so ergibt sich ebenso wie in §. 82 Gl. (4) und (3) für den Zähler

von $[a_0, a_1 \ldots a_m, c_1, c_2 \ldots c_r]$ der Ausdruck $c_{1,r} M_m + c_{2,r} M_{m-1}$

von $[a_0, a_1 \ldots a_m, c_1, c_2 \ldots c_r, 0]$ der Ausdruck $c_{1,r-1} M_m + c_{2,r-1} M_{m-1}$

und darauf für den Zähler

von $[a_0 \ldots a_m, c_1 \ldots c_r, 0, -b_n \ldots -b_1]$ der Ausdruck

$$(16)\qquad \begin{aligned}\overset{1}{M} = &[(-b)_{1,n} c_{1,r-1} + (-b)_{1,n-1} c_{1,r}] M_m \\ &+ [(-b)_{1,n} c_{2,r-1} + (-b)_{1,n-1} c_{2,r}] M_{m-1}\end{aligned}$$

Erzeugt man ebenso aus M_{m-1} und M_m den Werth von $\overset{-1}{M}$ aus (7); so erhält man für den Zähler

von $[a_0, a_1 \ldots a_m, 0, -c_r, -c_{r-1} \ldots -c_2]$ den Ausdruck
$(-c)_{2,r-1} M_m + (-c)_{2,r} M_{m-1}$

von $[a_0, a_1 \ldots a_m, 0, -c_r, -c_{r-1} \ldots -c_1]$ den Ausdruck
$(-c)_{1,r-1} M_m + (-c)_{1,r} M_{m-1}$

und darauf für den Zähler

von $[a_0, \ldots a_m, 0, -c_r \ldots -c_1, -b_n \ldots -b_1]$ den Ausdruck

$$(17)\qquad \begin{aligned}\overset{-1}{M} = &[(-b)_{1,n} (-c)_{1,r-1} + (-b)_{1,n-1} (-c)_{2,r-1}] M_m \\ &+ [(-b)_{1,n} (-c)_{1,r} + (-b)_{1,n-1} (-c)_{2,r}] M_{m-1}\end{aligned}$$

Multiplizirt man Gl. (17) mit $(-1)^{r-1}$, indem man beachtet, dass auf der rechten Seite $(-c)_{1,r-1}$ und $(-c)_{2,r}$ dasselbe Zeichen $(-1)^{r-1}$, ebenso $(-c)_{2,r-1}$ und $(-c)_{1,r}$ dasselbe Zeichen $(-1)^r$ besitzen; so ergibt sich durch Subtraktion der entstehenden Gleichung von Gl. (16)

$$\overset{1}{M} - (-1)^{r-1} \overset{-1}{M} = (c_{1,r} + c_{2,r-1}) [(-b)_{1,n-1} M_m + (-b)_{1,n} M_{m-1}]$$

Es ist aber offenbar nach Gl. (9)

$$c_{1,r} + c_{2,r-1} = \mathfrak{M}_{r-1} + \mathfrak{U}_{r-2} = h$$

und nach (3) oder (6)

$$(-b)_{1,n-1} M_m + (-b)_{1,n} M_{m-1} = \overset{0}{M}$$

Hierdurch wird die vorstehende Beziehung, wenn man $(-1)^{r-1} \overset{-1}{M}$ transponirt, wie zu beweisen war,

(18) $$\overset{1}{M} = h\overset{0}{M} + (-1)^{r-1}\overset{-1}{M}$$

IV. Nach Vorstehendem hat man folgende Rekursionsformel

für den Fortschritt in der Richtung der Zeiger $\ldots -2, -1, 0, 1, 2\ldots$	für den Rückschritt in der Richtung der Zeiger $\ldots 2, 1, 0, -1, -2\ldots$
$\overset{-2}{M} = h\overset{-3}{M} + (-1)^{r-1}\overset{-4}{M}$	$\overset{2}{M} = (-1)^r h\overset{3}{M} + (-1)^{r-1}\overset{4}{M}$
$\overset{-1}{M} = h\overset{-2}{M} + (-1)^{r-1}\overset{-3}{M}$	$\overset{1}{M} = (-1)^r h\overset{2}{M} + (-1)^{r-1}\overset{3}{M}$
$\overset{0}{M} = h\overset{-1}{M} + (-1)^{r-1}\overset{-2}{M}$	$\overset{0}{M} = (-1)^r h\overset{1}{M} + (-1)^{r-1}\overset{2}{M}$
$\overset{1}{M} = h\overset{0}{M} + (-1)^{r-1}\overset{-1}{M}$	$\overset{-1}{M} = (-1)^r h\overset{0}{M} + (-1)^{r-1}\overset{1}{M}$
$\overset{2}{M} = h\overset{1}{M} + (-1)^{r-1}\overset{0}{M}$	$\overset{-2}{M} = (-1)^r h\overset{-1}{M} + (-1)^{r-1}\overset{0}{M}$
$\overset{3}{M} = h\overset{2}{M} + (-1)^{r-1}\overset{1}{M}$	$\overset{-3}{M} = (-1)^r h\overset{-2}{M} + (-1)^{r-1}\overset{-1}{M}$
$\overset{4}{M} = h\overset{3}{M} + (-1)^{r-1}\overset{2}{M}$	$\overset{-4}{M} = (-1)^r h\overset{-3}{M} + (-1)^{r-1}\overset{-2}{M}$
$\vdots$	$\vdots$

(19) $\overset{n}{M} = h\overset{n-1}{M} + (-1)^{r-1}\overset{n-2}{M}$ (20) $\overset{n}{M} = (-1)^r h\overset{n+1}{M} + (-1)^{r-1}\overset{n+2}{M}$

Diese Formeln gelten auch für die entsprechenden Nenner N.

Nachdem man also aus (3) und (4) die Werthe $\overset{0}{K} = \dfrac{\overset{0}{M}}{\overset{0}{N}}$ und $\overset{1}{K} = \dfrac{\overset{1}{M}}{\overset{1}{N}}$ berechnet hat, ergeben sich die Glieder der obigen beiden Systeme nach den vorstehenden Formeln wie eine einzige zusammenhängende Reihe, welche man nach unten und nach oben beliebig weit fortsetzen kann.

V. Beispiel. Es seien zu kombiniren

$K = [1, 1, \underbrace{3, 6}, \underbrace{3, 6}\ldots]$ und $K' = [0, 1, \underbrace{3, 6}, \underbrace{3, 6}\ldots]$

n	P_n	Q_n	a_n	n	P_n	Q_n	a_n
-1		-10		-1		1	
0	9	7	1	0	2	7	0
1	-2	1	1	1	-2	1	1
2	3	2	3	2	3	2	3
3	3	1	6	3	3	1	6
4	3	2	3	4	3	2	3
5	3	1	6	5	3	1	6

Die beiden Systeme sind hier

K (2), (4), (6), (8)... *komb.* K' (2) und K (2) *komb.* K' (2), (4), (6), (8)...

und man hat

$$\overset{0}{K}=\frac{\overset{0}{M}}{\overset{0}{N}}=[1,\ 1,\ 0,\ -1]=\frac{1}{0}$$

$$\overset{1}{K}=\frac{\overset{1}{M}}{\overset{1}{N}}=[1,\ 1,\ 3,\ 6,\ 0,\ -1]=\frac{37}{21}$$

$$\mathfrak{K}_{r-1}=\frac{\mathfrak{M}_{r-1}}{\mathfrak{N}_{r-2}}=[\bar{3},\ 6]=\frac{19}{6},\ \frac{\mathfrak{M}_{r-2}}{\mathfrak{N}_{r-2}}=\frac{3}{1}$$

$$h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}=19+1=20$$

$$r=2,\ (-1)^r=+1,\ (-1)^{r-1}=-1$$

also statt Gl. (20) und (19)

$$\overset{n}{M}=20\overset{n+1}{M}-\overset{n+2}{M} \qquad \overset{n}{N}=20\overset{n+1}{N}-\overset{n+2}{N}$$

$$\overset{n}{M}=20\overset{n-1}{M}-\overset{n-2}{M} \qquad \overset{n}{N}=20\overset{n-1}{N}-\overset{n-2}{N}$$

Dies gibt folgende Rechnung

n	h	$\overset{n}{M}$	$\overset{n}{N}$
-4	20	-167160	-135719
-3	20	-8379	-6803
-2	20	-420	-341
-1	20	-21	-17
0		0	1
1		21	37
2	20	420	739
3	20	8379	14743
4	20	167160	294121
5	20	3334821	5867677

§. 85. *Rekursionsformel für die in einem bestimmten gegenseitigen Abstande liegenden Glieder der soeben betrachteten Reihe.*

I. Bei dem allgemeinsten Falle der unbestimmten Gleichungen vom zweiten Grade kommt es nicht darauf an, alle, sondern gewisse in einem bestimmten gegenseitigen Abstande liegende Glieder der im vorhergehenden Paragraphen betrachteten Grössenreihen zu bestimmen. Wir wollen jetzt die Rekursionsformel aufstellen, mittelst welcher man die überflüssige Berechnung der nicht verlangten Glieder vermeiden kann.

Es sei n der Zeiger Eines der zu berechnenden Glieder und s der gegenseitige Abstand der Letzteren, sodass also die Zähler und Nenner der Grössen

$$\ldots\overset{n-3s}{K}\quad\overset{n-2s}{K}\quad\overset{n-s}{K}\quad\overset{n}{K}\quad\overset{n+s}{K}\quad\overset{n+2s}{K}\quad\overset{n+3s}{K}\ldots$$

zu berechnen sind. Wir nehmen an, zwei benachbarte Grössen $\overset{n}{K}$ und $\overset{n+s}{K}$ seien bereits durch die Methode des vorhergehenden Paragraphen dargestellt, und es handele sich darum, mit Hülfe dieser die übrigen zu finden.

Die Zähler M, sowie die Nenner N sind an die bekannte Beziehung

(1) $$\overset{n}{M} = h\overset{n-1}{M} + (-1)^{r-1}\overset{n-2}{M} = h\overset{n-1}{M} \pm \overset{n-2}{M}$$

gebunden.

II. Bilden wir jetzt nach der Grundregel für die Erzeugung der Zähler der Näherungswerthe eines Kettenbruchs die nachfolgenden Grössen h_{-1}, h_0, h_1, $h_2 \ldots$ aus dem Kettenbruche $[h, h, h, h, h \ldots]$ sowol nach dem Additions- wie nach dem Subtraktionsprinzipe

$$\begin{array}{lll} & 0 & = h_{-1} \\ & 1 & = h_0 \\ h & h & = h_1 \\ h & h^2 \pm 1 & = h_2 \\ h & h^3 \pm 2h & = h_3 \\ h & h^4 \pm 3h^2 + 1 & = h_4 \\ h & h^5 \pm 4h^3 + 3h & = h_5 \\ h & h^6 \pm 5h^4 + 6h^2 \pm 1 & = h_6 \\ h & h^7 \pm 6h^5 + 10h^3 \pm 4h & = h_7 \end{array}$$

u. s. w., wobei sich die oberen Zeichen auf das Additions- und die unteren auf das Subtraktionsprinzip beziehen; so findet man leicht allgemein, wenn

$$\overset{p}{B}_q = \frac{p(p-1)(p-2)\ldots(p-q+1)}{1 .\ 2 ..\ \ 3\ \ \ldots\ \ q}$$

den $q$ten Binomialkoeffizienten der $p$ten Potenz bezeichnet

(2) $$h_n = h^n \pm \overset{n-1}{B_1} h^{n-2} + \overset{n-2}{B_2} h^{n-4} \pm \overset{n-3}{B_3} h^{n-6} + \overset{n-4}{B_4} h^{n-8} \pm \text{etc.}$$

Diese Reihe setzt sich, wenn n paar ist, so weit fort, bis der Exponent von h gleich 0 wird, und wenn n unpaar ist, so weit, bis dieser Exponent gleich 1 wird.

III. Setzen wir

(3) $$H = h^s \pm sh^{s-2} + \frac{s(s-3)}{1 . 2} h^{s-4} \pm \frac{s(s-4)(s-5)}{1 .\ 2 .\ \ 3} h^{s-6}$$
$$+ \frac{s(s-5)(s-6)(s-7)}{1 .\ 2 .\ \ 3 .\ \ 4} h^{s-8} \pm \text{etc.}$$
$$= h^s \pm sh^{s-2} + \frac{s}{2}\overset{s-3}{B_1} h^{s-4} \pm \frac{s}{3}\overset{s-4}{B_2} h^{s-6} + \frac{s}{4}\overset{s-5}{B_3} h^{s-8} \pm \text{etc.}$$

indem wir die Glieder dieser Reihe, wenn s paar ist, so weit nehmen, bis der Exponent von h gleich 0 wird, und wenn s unpaar ist, so weit, bis dieser Exponent $= 1$ wird; so lässt sich, welches auch der Werth von n sei, leicht die Richtigkeit der Gleichung

(4) $$h_{n+2s} = Hh_{n+s} - (\mp 1)^s h_n$$

konstatiren, worin resp. das obere oder untere Zeichen gilt, jenachdem in den vorhergehenden Gleichungen das obere oder, untere Zeichen stattfindet. Hieraus folgt auch

$$(5) \qquad H = \frac{h_{n+2s} + (\mp 1)^s h_n}{h_{n+s}}$$

Nimmt man hierin einmal $n = -1$; so ergibt sich, da $h_{-1} = 0$ ist, zur Berechnung der Grösse H die zweite Formel

$$(6) \qquad H = \frac{h_{2s-1}}{h_{s-1}} \quad .$$

IV. Eine Substitution dieses Werthes von H in die Gl. (4) liefert auch die Beziehung

$$(7) \qquad h_{2s-1} h_{s+n} - h_{s-1} h_{2s+n} = (\mp 1)^s h_{s-1} h_n$$

und für $n = 0$, da $h_0 = 1$ ist,

$$(8) \qquad h_s h_{2s-1} - h_{s-1} h_{2s} = (\mp 1)^s h_{s-1}$$

Es muss auch noch bemerkt werden, dass man in den Formeln (4), (5), (7) für n auch negative Zeiger zulassen kann. Für solche Zeiger verliert jedoch die Gl. (2) ihre Bedeutung, indem die rückwärts gerichtete Fortsetzung des obigen Bildungsgesetzes der Grössen h_n folgende Werthe ergibt

$$h \quad -(h^5 \pm 4h^3 + 3h) = h_{-7} = -h_5$$
$$h \quad \pm(h^4 \pm 3h^2 + 1) = h_{-6} = \pm h_4$$
$$h \quad -(h^3 \pm 2h) = h_{-5} = -h_3$$
$$h \quad \pm(h^2 \pm 1) = h_{-4} = \pm h_2$$
$$h \quad -h = h_{-3} = -h_1$$
$$h \quad \pm 1 = h_{-2} = \pm h_0$$
$$h \quad 0 = h_{-1}$$
$$h \quad 1 = h_0$$
$$h \quad h = h_1$$

u. s. w.

V. Was nun die gesuchten Werthe von M betrifft; so findet sich sofort ganz allgemein

$$(9) \qquad \overset{n}{M} = h_{n-1} \overset{1}{M} \pm h_{n-2} \overset{0}{M} \text{ also}$$

$$(10) \qquad \overset{n+s}{M} = h_{n+s-1} \overset{1}{M} \pm h_{n+s-2} \overset{0}{M} \text{ und}$$

$$(11) \qquad \overset{n+2s}{M} = h_{n+2s-1} \overset{1}{M} \pm h_{n+2s-2} \overset{0}{M}$$

Substituirt man in die letzte Gleichung für h_{n+2s-1} und h_{n+2s-2} ihre aus Gl. (4) sich ergebenden Werthe; so kommt

$$\overset{n+2s}{M} = [H h_{n+s-1} - (\mp 1)^s h_{n-1}] \overset{1}{M} \pm [H h_{n+s-2} - (\mp 1)^s h_{n-2}] \overset{0}{M}$$
$$= H [h_{n+s-1} \overset{1}{M} \pm h_{n+s-2} \overset{0}{M}] - (\mp 1)^s [h_{n-1} \overset{1}{M} \pm h_{n-2} \overset{0}{M}]$$

d. i. wegen der Werthe aus (10) und (9)

$$(12) \qquad \overset{n+2s}{M} = H \overset{n+s}{M} - (\mp 1)^s \overset{n}{M}$$

Da in dieser Gleichung das Zeichen ∓ 1 gilt, jenachdem man $(-1)^{r-1} = \pm 1$ hat; so ist $\mp 1 = -(\pm 1) = -(-1)^{r-1} = (-1)^r$ also $(\mp 1)^s = (-1)^{rs}$ und $-(\mp 1)^s = (-1)^{rs-1}$ zu setzen, wodurch die vorstehende Gleichung

(13) $$\overset{n+2s}{M} = H\overset{n+s}{M} + (-1)^{rs-1}\overset{n}{M}$$

wird.

Das gesuchte Bildungsgesetz ist hiernach das folgende

für den Fortschritt in der Richtung der Zeiger $\ldots n-2s,\ n-s,\ n,\ n+s,\ n+2s\ldots$	für den Rückschritt in der Richtung der Zeiger $\ldots n+2s,\ n+s,\ n,\ n-s,\ n-2s\ldots$
$\overset{n-s}{M} = H\overset{n-2s}{M} + (-1)^{rs-1}\overset{n-3s}{M}$	$\overset{n+s}{M} = (-1)^{rs}H\overset{n+2s}{M} + (-1)^{rs-1}\overset{n+3s}{M}$
$\overset{n}{M} = H\overset{n-s}{M} + (-1)^{rs-1}\overset{n-2s}{M}$	$\overset{n}{M} = (-1)^{rs}H\overset{n+s}{M} + (-1)^{rs-1}\overset{n+2s}{M}$
$\overset{n+s}{M} = H\overset{n}{M} + (-1)^{rs-1}\overset{n-s}{M}$	$\overset{n-s}{M} = (-1)^{rs}H\overset{n}{M} + (-1)^{rs-1}\overset{n+s}{M}$
$\overset{n+2s}{M} = H\overset{n+s}{M} + (-1)^{rs-1}\overset{n}{M}$	$\overset{n-2s}{M} = (-1)^{rs}H\overset{n-s}{M} + (-1)^{rs-1}\overset{n}{M}$
$\overset{n+3s}{M} = H\overset{n+2s}{M} + (-1)^{rs-1}\overset{n+s}{M}$	$\overset{n-3s}{M} = (-1)^{rs}H\overset{n-2s}{M} + (-1)^{rs-1}\overset{n-s}{M}$

Diese Formeln gelten auch für die Nenner N. Um dieselben in Anwendung zu bringen, braucht man nicht einmal die Grössen M, N von den Zeigern n und $n+s$, sondern nur die von den Zeigern 0 und 1 als bekannt vorauszusetzen, indem die ersteren nach Gl. (9) und (10) berechnet werden können.

VI. Beispiel. Es sollen aus dem Beispiele des §. 84 die Grössen von den Zeigern $\ldots -7,\ -4,\ -1,\ 2,\ 5,\ 8\ldots$ bestimmt werden.

Man hat hierfür $\dfrac{\overset{-1}{M}}{\overset{-1}{N}} = \dfrac{-21}{-17},\ \dfrac{\overset{2}{M}}{\overset{2}{N}} = \dfrac{420}{739},\ n = -1,\ s = 3.$

Da $h = 20$ ist; so hat man zur Berechnung der Grösse H nach Gl. (6) aus $h_{s-1} = h_2$ und $h_{2s-1} = h_5$, indem man wegen $r = 2$ also $(-1)^{r-1} = -1$ auf den Kettenbruch $[h, h, h\ldots]$ $= [20, 20, 20\ldots]$ das Subtraktionsprinzip in Anwendung bringt

	$0 = h_{-1}$
	$1 = h_0$
20	$20 = h_1$
20	$399 = h_2$
20	$7960 = h_3$
20	$158801 = h_4$
20	$3168060 = h_5$

$$H = \frac{h_{2s-1}}{h_{s-1}} = \frac{h_5}{h_2} = \frac{3168060}{399} = 7940$$

Nach der Formel (3) würde man die einfachere Rechnung

$$H = 20^3 - 3.20 = 7940$$

haben.

Da hier nun $rs = 2.3 = 6$, also $(-1)^{rs-1} = (-1)^5 = -1$ und $(-1)^{rs} = +1$ ist; so erhält man für die vorwärtsschreitende Bildung

$$\overset{3v-1}{M} = 7940\overset{3v-4}{M} - \overset{3v-7}{M} \qquad \overset{3v-1}{N} = 7940\overset{3v-4}{N} - \overset{3v-7}{N}$$

und für die **rückwärts**schreitende Bildung

$$\overset{3\nu-1}{M} = 7940\,\overset{3\nu+2}{M} - \overset{3\nu+5}{M} \qquad \overset{3\nu-1}{N} = 7940\,\overset{3\nu+2}{N} - \overset{3\nu+5}{N}$$

welche beide im **Subtraktionsprinzipe** liegen. Dies gibt folgende Rechnung

n	H	$\overset{n}{M}$	$\overset{n}{N}$
-4	7940	-167160	-135719
-1	7940	-21	-17
2	7940	420	739
5	7940	3334821	5867677

§. 86. Reste der Grössen $\overset{n}{M}$ und $\overset{n}{N}$.

I. Die im vorhergehenden Paragraphen betrachteten Grössen M, N von den Zeigern $\ldots n-2s,\ n-s,\ n,\ n+s,\ n+2s \ldots$ bilden eine engere Auswahl unter den Grössen von den Zeigern $\ldots -2, -1, 0, 1, 2 \ldots$ Bei den unbestimmten Gleichungen vom zweiten Grade wird diese Auswahl unter der Bestimmung zu treffen sein, dass jede Grösse Ein und derselben Reihe, z. B., jede Grösse der Reihe $\ldots \overset{n-2s}{M}, \overset{n-s}{M}, \overset{n}{M}, \overset{n+s}{M}, \overset{n+2s}{M} \ldots$ nachdem man dieselbe um eine konstante Grösse A vermehrt oder vermindert hat, durch eine andere gegebene Grösse p **theilbar** werde. Es soll also

$$(1) \qquad \frac{M-A}{p} = q \text{ oder } M - A = pq$$

sein, worin q eine **ganze** Zahl bedeutet. Hierin kann q ebenso wie M, A, p sowol positiv wie negativ sein; man wird übrigens, wenn q positiv oder negativ gedacht wird, p stets als positiv voraussetzen dürfen.

Wenn man nach den Regeln der gewöhnlichen Division mit p in M und auch in A dividirt und dabei die grössten Subquotienten nimmt, sodass die **Reste** dieser Divisionen entschieden **positiv** und **kleiner** als der absolute Werth des Divisors p sind; so erfordert die Bedingung (1) offenbar die **Gleichheit** der eben erwähnten beiden Reste. Demnach sind die Grössen M aus der fraglichen Reihe unter der Bedingung auszusuchen, dass ihre positiven Reste in Beziehung zum Divisor p gleich dem Reste der gegebenen Grösse A in Beziehung zu demselben Divisor seien.

Zur Abkürzung der Bezeichnung bedienen wir uns des Kongruenzzeichens $\equiv$, um durch die Formel $a \equiv b$ auszudrücken, dass die beiden ganzen Zahlen a und b sich nur durch irgend ein Vielfaches einer gewissen Zahl p voneinander unterscheiden. Jene Formel ist also gleichbedeutend mit der Gleichung $a = wp + b$, worin w eine beliebige positive oder negative ganze Zahl bezeichnet.

II. Denken wir uns nun die vorhin genannten kleinsten positiven Reste der Grössen $\overset{n}{M}$ in Beziehung zu dem Divisor p gebildet, indem wir dieselben entsprechend mit $\overset{n}{R}$ bezeichnen.

Beachtet man, dass die Grössen $\overset{n}{M}$ aus den gegebenen Werthen $\overset{0}{M}$, $\overset{1}{M}$ und h nach der Rekursionsformel

$$(2) \qquad \overset{n}{M} = h\overset{n-1}{M} + (-1)^{r-1}\overset{n-2}{M} = h\overset{n-1}{M} \pm \overset{n-2}{M}$$

entstehen; so ist es offenbar nicht nöthig, erst alle Grössen M herzustellen, und eine jede durch p zu dividiren, um die Reste R zu finden: man kann vielmehr gleich von vorn herein, um mit möglichst kleinen und positiven Zahlen zu thun zu haben, für jede der ursprünglich gegebenen Grössen h, $\overset{0}{M}$, $\overset{1}{M}$, wenn dieselbe positiv und $\geqq p$, oder wenn dieselbe negativ sein sollte, ihren kleinsten Rest in Beziehung zu p an die Stelle setzen. Ausserdem kann man für jede der durch die Formel (2) erzeugten Grössen bei der Fortsetzung der Rechnung ihren kleinsten Rest nehmen.

So ergibt sich z. B. für $p = 7$, $h = 24$, $\overset{0}{M} = 5$, $\overset{1}{M} = -12$, wenn in der Formel (2) das Additionsprinzip gilt, indem man $h = 3.7 + 4 \equiv 4$, $\overset{1}{M} = -2.7 + 2 \equiv 2$ setzt,

	$\overset{0}{M} = 5 \equiv 5 \ldots \overset{0}{R}$	4	$\overset{8}{M} \equiv 16 \equiv 2 \ldots \overset{8}{R}$
	$\overset{1}{M} = -12 \equiv 2 \ldots \overset{1}{R}$	4	$\overset{9}{M} \equiv 12 \equiv 5 \ldots \overset{9}{R}$
$h \equiv 4$	$\overset{2}{M} \equiv 13 \equiv 6 \ldots \overset{2}{R}$	4	$\overset{10}{M} \equiv 22 \equiv 1 \ldots \overset{10}{R}$
4	$\overset{3}{M} \equiv 26 \equiv 5 \ldots \overset{3}{R}$	4	$\overset{11}{M} \equiv 9 \equiv 2 \ldots \overset{11}{R}$
4	$\overset{4}{M} \equiv 26 \equiv 5 \ldots \overset{4}{R}$	4	$\overset{12}{M} \equiv 9 \equiv 2 \ldots \overset{12}{R}$
4	$\overset{5}{M} \equiv 25 \equiv 4 \ldots \overset{5}{R}$	4	$\overset{13}{M} \equiv 10 \equiv 3 \ldots \overset{13}{R}$
4	$\overset{6}{M} \equiv 21 \equiv 0 \ldots \overset{6}{R}$	4	$\overset{14}{M} \equiv 14 \equiv 0 \ldots \overset{14}{R}$
4	$\overset{7}{M} \equiv 4 \equiv 4 \ldots \overset{7}{R}$	4	$\overset{15}{M} \equiv 3 \equiv 3 \ldots \overset{15}{R}$
		4	$\overset{16}{M} \equiv 12 \equiv 5 \ldots \overset{16}{R}$
u. s. w.		4	$\overset{17}{M} \equiv 23 \equiv 2 \ldots \overset{17}{R}$

Da alle diese Reste $< p$ sind; so ist nicht bloss klar, dass sich an irgend einer Stelle Ein schon früher vorgekommener Rest, sondern dass sich an irgend einer Stelle zwei schon früher vorgekommene benachbarte Reste in derselben Reihenfolge wiederholen müssen. Von dieser Stelle an werden

sich dann aber wegen des Bildungsgesetzes (2) alle folgenden Reste in derselben Reihenfolge wiederholen. Da nun das Gesetz (2) eine Umkehrung gestattet, wonach jedes frühere Glied aus den beiden späteren nach derselben Regel erzeugt wird; so leuchtet ein, dass sich alle Reste vom oberen $\overset{0}{R}$ an in regelmässigen Perioden wiederholen werden.

Demnach braucht man, um alle möglichen verschiedenen Reste zu finden, nur so weit zu rechnen, bis sich die ersten beiden Reste $\overset{0}{R}$, $\overset{1}{R}$ wieder einstellen.

Im obigen Beispiele wiederholen sich die ersten beiden Reste $\overset{0}{R}=5$ und $\overset{1}{R}=2$ bei $\overset{16}{R}$ und $\overset{17}{R}$; die Periode schliesst also mit $\overset{15}{R}$ und hat 16 Glieder.

III. Wenn es sich ereignet, dass zwei benachbarte Reste $\overset{n}{R}$, $\overset{n+1}{R}$ erscheinen, welche sich resp. mit $\overset{0}{R}$, $\overset{1}{R}$ zu p ergänzen; so ergänzen sich auch alle auf $\overset{n+1}{R}$ folgenden mit den auf $\overset{1}{R}$ folgenden zu p.

Denn wenn man hat

$\overset{n}{R} = p - \overset{0}{R}$

$\overset{n+1}{R} = p - \overset{1}{R}$; so ist auch der folgende Rest

$$\overset{n+2}{R} \equiv h(p - \overset{1}{R}) \pm (p - \overset{0}{R}) \equiv -(h\overset{1}{R} \pm \overset{0}{R}) \equiv -\overset{2}{R} \equiv p - \overset{2}{R}$$

also da $\overset{n+2}{R} < p$ ist, $\overset{n+2}{R} = \overset{2}{R}$ u. s. f.

Dies ereignet sich im obigen Beispiele, indem

$$\overset{8}{R} = 2 = 7 - 5 = p - \overset{0}{R} \text{ und } \overset{9}{R} = 5 = 7 - 2 = p - \overset{1}{R} \text{ ist.}$$

In einem solchen Falle also, wo die Ergänzungen von $\overset{0}{R}$ und $\overset{1}{R}$ zu p wiederkehren, kann man von dieser Stelle an die folgenden Reste dadurch leicht erzeugen, dass man die schon berechneten von p subtrahirt.

Es ist klar, dass nach der umgekehrten Rekursionsformel

(3) $\overset{n}{M} = (-1)^r h \overset{n+1}{M} + (-1)^{r-1} \overset{n+2}{M} = (-1)^{r-1} (-h \overset{n+1}{M} + \overset{n+2}{M})$

welche für die Grössen M gilt, auch die Reste R von jedem Gliede an, also auch vom Gliede $\overset{0}{R}$ an, rückwärts gebildet werden können.

IV. Wenn es sich ereignet, dass man auf einen Rest $\overset{n}{R} = 0$ stösst; so tritt für die folgenden Reste die nachstehende Beziehung ein, welche wir der Kürze halber nur für das Additionsprinzip konstatiren wollen, welche aber mit Hülfe der Gl. (2) und (3) leicht allgemein erwiesen werden kann.

$\overset{n}{R} = 0$

$\overset{n+1}{R} \equiv h\overset{n}{R} + \overset{n-1}{R} \equiv \overset{n-1}{R}$

$\overset{n+2}{R} \equiv h\overset{n-1}{R} + \overset{n}{R} \equiv h\overset{n-1}{R}$ (also da aus $\overset{n}{R} \equiv h\overset{n-1}{R} + \overset{n-2}{R}$ die Beziehung $h\overset{n-1}{R} \equiv -\overset{n-2}{R}$ folgt)

$\equiv -\overset{n-2}{R} \equiv p - \overset{n-2}{R}$

$\overset{n+3}{R} \equiv -h\overset{n-2}{R} + \overset{n-1}{R} \equiv \overset{n-3}{R}$

$\overset{n+4}{R} \equiv h\overset{n-3}{R} - \overset{n-2}{R} \equiv -(-h\overset{n-3}{R} + \overset{n-2}{R}) \equiv -\overset{n-4}{R} \equiv p - \overset{n-4}{R}$

u. s. w. Die Reihe der Reste hinter der fraglichen Stelle befolgt also dieses Gesetz

Zeiger	$= n$	$n+1$	$n+2$	$n+3$	$n+4$	$n+5$	$n+6$	...
Rest	$= 0$	$\overset{n-1}{R}$	$(p - \overset{n-2}{R})$	$\overset{n-3}{R}$	$(p - \overset{n-4}{R})$	$\overset{n-5}{R}$	$(p - \overset{n-6}{R})$	...

wonach dieselbe leicht bis $\overset{n+n}{R} = \overset{2n}{R}$ fortgeführt werden kann. So hat man im obigen Beispiele für $n = 6$

$n = \ldots$	2	3	4	5	6	7	8	9	10	...
$\overset{n}{R} = \ldots$	6	5	5	4	0	4	(7−5)	5	(7−6)	...

Da sich jeder Rest wiederholt; so wiederholt sich auch der Rest 0. Aus Vorstehendem erhellet, dass wenn man bei der Berechnung der Reste R zweimal den Werth 0 erhalten hat (was nicht nothwendig in einem Abstande von der Länge der Periode zu geschehen braucht, sondern in einem kürzeren Abstande geschehen kann), man alle folgenden Reste bis zum Schlusse der Periode nicht nach der Formel (2) zu bilden nöthig hat, vielmehr durch einfache Wiederholung der rückwärts laufenden Reihe der schon gebildeten Reste und deren Ergänzungen zu p, in abwechselndem Turnus.

V. Die Länge der Periode der Reste R in Beziehung zu einem gegebenen Divisor p ist im Allgemeinen unabhängig von den Grössen $\overset{0}{M}$ und $\overset{1}{M}$. Sie ist entweder ebenso gross, wie die Periodenlänge der Grössen ... h_{-1}, h_0, h_1, h_2 ... (§. 85), welche nach einem ähnlichen Gesetze gebildet sind, wie die Grössen M, indem man für die ersteren derselben $h_{-1} = 0$, $h_0 = 1$, $h_1 = h$, $h_2 = h^2 + 1$ u. s. w. hat, oder sie ist gleich einem aliquoten Theile der letzteren Periodenlänge.

Denn bezeichnet man den Rest von h_n in Beziehung zu demselben Divisor p mit r_n, und enthält die Periode der letzteren Grössen n Glieder, sodass sich also die Reste ... $r_{-2}, r_{-1}, r_0, r_1, r_2$ ... bei ... $r_{n-2}, r_{n-1}, r_n, r_{n+1}, r_{n+2}$ ... wiederholen; so wiederholen sich auch die Reste R der Grössen M bei denselben Zeigern, indem man hat

$$\overset{n}{R} \equiv r_{n-1} \overset{1}{R} + r_{n-2} \overset{0}{R} \equiv r_{-1} \overset{1}{R} + r_{-2} \overset{0}{R} \equiv \overset{0}{R}$$

$$\overset{n+1}{R} \equiv r_n \overset{1}{R} + r_{n-1} \overset{0}{R} \equiv r_0 \overset{1}{R} + r_1 \overset{0}{R} \equiv \overset{1}{R}$$

u. s. w. Hiernach, wo die Reste in Abständen von n Gliedern nothwendig wiederkehren müssen, ist klar, dass wenn in besonderen Fällen die regelmässige Wiederkehr schon früher eintreten sollte, Dies nur in Abständen geschehen kann, deren Gliederzahl ein aliquoter Theil von n ist.

VI. Es bedarf keines weiteren Nachweises, dass wenn man die Grössen M mit einer konstanten Zahl c multiplizirt und auch dem Produkte noch eine konstante Zahl d hinzufügt, die Reste der Grössen $cM + d$ ebenfalls Perioden bilden werden. Und zwar ist die Periode von $cM + d$ ebenso lang, wie die von cM. Die Periodenlänge von cM kann jedoch, wenn sie der von M nicht gleich ist, nur ein aliquoter Theil der letzteren sein.

VII. Nach Obigem ist es leicht, diejenigen Reihen der M zu bezeichnen, welche sämmtlich denselben Rest besitzen oder der Bedingung (1) entsprechen.

Besitzt nämlich die Periode der Reste s Glieder; so entspricht jedem $\overset{n}{R}$ in der ersten Periode, welches den verlangten Werth besitzt, die Reihe

$$\ldots \overset{n-2s}{M}\ \overset{n-s}{M}\ \overset{n}{M}\ \overset{n+s}{M}\ \overset{n+2s}{M} \ldots$$

Soll im obigen Beispiele $\frac{M-A}{p} = \frac{M-25}{7} = \frac{M-(3.7+4)}{7}$, also auch $\frac{M-4}{7} = q$ eine ganze Zahl oder der fragliche Rest $\overset{n}{R} = 4$ sein; so findet man in der ersten Periode, welche $s = 16$ Glieder besitzt, sowol $\overset{5}{R} = 4$, wie auch $\overset{7}{R} = 4$. Dies gibt folgende zwei Reihen

$$\ldots \overset{-27}{M}\ \overset{-11}{M}\ \overset{5}{M}\ \overset{21}{M}\ \overset{37}{M} \ldots$$

$$\ldots \overset{-25}{M}\ \overset{-9}{M}\ \overset{7}{M}\ \overset{23}{M}\ \overset{39}{M} \ldots$$

Kommt in der ersten Periode der gesuchte Rest nicht vor; so gibt es überhaupt Grössen M von der verlangten Eigenschaft nicht.

VIII. Was hier von den Zählern M gesagt ist, gilt auch von den Nennern N. Bei den unbestimmten Gleichungen wird es darauf ankommen, diejenigen M und N von gleichen Zeigern zu bestimmen, von denen die ersteren einen bestimmten Rest A und die letzteren gleichzeitig einen bestimmten Rest B haben. Es ist möglich, dass es sowol Reihen für M, wie auch Reihen für N gibt, welche für sich allein der gegebenen Bedingung entsprechen, welche aber nicht gleiche Zeiger haben. Unter solchen Umständen würde die Aufgabe immerhin unmöglich sein.

Die Möglichkeit oder Unmöglichkeit der letzteren Aufgabe kann man aber jederzeit an den Resten von M und N der ersten Periode beurtheilen. Man beachte nämlich, dass wenn s die Gliederzahl der Periode der Reste der Grössen h_n ist, die Gliederzahlen s' und s'' der Perioden von M und N irgend welche aliquote Theile von s sind. Nimmt man also sowol die Periode von M, wie auch die von N auf die Länge s oder auch nur so weit, bis gleichzeitig die Reste von M und die von N sich wiederholen; so liefern nur diejenigen in dieser grösseren Periode liegenden Zeiger n, für welche gleichzeitig $\overset{n}{M} \equiv A$ und $\overset{n}{N} \equiv B$ ist, gesuchte Reihen. Denn wäre in dieser Periode für den Zeiger n' die Grösse $M \equiv A$ und für einen anderen Zeiger n'' die Grösse $N \equiv B$; so kann für keinen ausserhalb jener Periode liegenden Zeiger n die Grösse $\overset{n}{M} \equiv A$ und zugleich $\overset{n}{N} \equiv B$ werden, weil sonst gleichzeitig $n = n' + xs$ und $n = n'' + ys$ also

$$n' + xs = n'' + ys \quad \text{folglich}$$

$$x - y = \frac{n'' - n'}{s}$$

sein müsste, was, weil $n'' - n'$ jedenfalls $< s$ ist, nur für $n'' = n'$ möglich sein würde.

Um die zusammengehörigen Werthe von M und N zu finden, ist es übrigens nicht durchaus nothwendig, die Perioden der Reste dieser Grössen auf eine gleiche Länge s zu erweitern, insofern die kleinsten Perioden verschiedene Längen s' und s'' haben sollten. Man kann nämlich für jede zwei Zeiger n' und n'' in diesen kürzesten Perioden, wofür $M \equiv A$ und $N \equiv B$ ist, untersuchen, ob die Gleichung

$$n = n' + xs' = n'' + ys'' \quad \text{oder}$$

$$s'x - s''y = n'' - n'$$

möglich ist. Diese Gleichung, welche in Beziehung zu x und y eine diophantische vom ersten Grade mit zwei Unbekannten ist, wird dann und auch nur dann möglich sein, wenn eine Befreiung der drei Zahlen s', s'', $(n'' - n')$ von ihrem etwaigen gemeinschaftlichen Maasse zwei relativ prime Koeffizienten von x und y zurücklässt (§. 27). Ist diese Gleichung möglich; so erscheint die Auflösung in der Form

$$x = a' + b'w \qquad y = a'' + b''w$$

und man hat dann

$$n = n' + a's' + b's'w = n'' + a''s'' + b''s''w$$

worin $b's' = b''s'' = s$ sein wird, sodass man für die ersten Glieder der vorwärts und rückwärts um je s Glieder fortschreitenden gesuchten Reihe

$$\overset{n'+a's'}{M} \equiv A \qquad \overset{n''+a''s''}{N} \equiv B$$

hat.

Fall, wo die Determinante ein vollkommenes Quadrat, verschieden von null, ist.

§. 87. *Entwickelung der Grösse $K=\frac{\sqrt{a^2}+P_0}{Q_0}$, worin die Determinante $D=a^2$ ein vollkommenes Quadrat ist, in einen Kettenbruch.*

I. Es leuchtet ein, dass in diesem Falle, wo K einen rationalen Werth $\frac{a+P_0}{Q_0}$ hat, die Entwickelung von K in einen Kettenbruch, wenn man dabei ein bestimmtes Prinzip, wie das Additionsprinzip mit grössten Subquotienten, zu Grunde legt, keine anderen Quotienten erzeugen kann, als diejenigen, welche sich nach demselben Prinzipe durch die Entwickelung von $\frac{a+P_0}{Q_0}$ ergeben würden, dass also diese Entwickelung eine endliche Länge haben wird. Bei der gegenwärtigen Untersuchung kommt es uns jedoch nicht allein auf diese Quotienten von K, sondern auch auf die Grössen P, Q an. Diese Letzteren ergeben sich nun genau nach der Vorschrift des §. 59, indem man in der ganzen Rechnung die Grösse $\sqrt{a^2}$ in dieser Form an alle den Stellen beibehält, wo man früher die Grösse $\sqrt{D}$ stehen hatte. Es wird noch bemerkt, dass auch hier die frühere Voraussetzung, wonach $\frac{a^2-P_0^2}{Q_0}=Q_{-1}$ eine ganze Zahl sein soll, gemacht wird.

So hat man z. B. für $K=\frac{\sqrt{16}+7}{3}$, worin $D=16=4^2$, $a=4$, $Q_{-1}=\frac{16-7^2}{3}=-11$ ist,

$$x_0=\frac{\sqrt{16}+7}{3}=3+\frac{1}{x_1}$$

$$x_1=\frac{3}{\sqrt{16}-2}=\frac{3(\sqrt{16}+2)}{12}=\frac{\sqrt{16}+2}{4}=1+\frac{1}{x_2}$$

$$x_2=\frac{4}{\sqrt{16}-2}=\frac{4(\sqrt{16}+2)}{12}=\frac{\sqrt{16}+2}{3}=2+\frac{1}{x_3}$$

$$x_3=\frac{3}{\sqrt{16}-4}=\frac{3(\sqrt{16}+4)}{0}=\frac{\sqrt{16}+4}{0}$$

also $K=\frac{\sqrt{16}+7}{3}=\frac{11}{3}=[3, 1, 2]$ und

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-11		1	0
0	7	3	3	3	1
1	2	4	1	4	1
2	2	3	2	11	3
3	4	0			

II. Wollte man die Entwickelung über den letzten Zeiger 3, für welchen $Q_3 = 0$ geworden ist, mit grössten Subquotienten fortsetzen; so würde, da $x_3 = \frac{\sqrt{16}+4}{0} = \infty$ ist, der nächste Quotient $a_3 = \infty$ werden, und Dies würde, wenn auch nicht für P und Q, doch für alle folgenden Werthe der Zähler M und Nenner N der Näherungsbrüche, zu unendlich grossen Zahlen führen, welche wir von unserer Betrachtung ganz ausschliessen wollen.

Demnach ist die Entwickelung mit grössten Subquotienten abzubrechen, sobald sich für x_n der Werth ∞ einstellt. Für den speziellen Fall $K = \sqrt{a^2}$ geschieht Dies immer schon bei dem Zeiger $n = 1$, indem man für $K = \sqrt{a^2} = \frac{\sqrt{a^2}+0}{1}$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		a^2		1	0
0	0	1	a	a	1
1	a	0			

hat. Aber auch in jedem anderen Falle muss sich jener Umstand ereignen, sobald nur die Determinante ein vollkommenes Quadrat ist. Für diesen Zeiger n aber, wo $Q_n = \frac{D - P_n^2}{Q_{n-1}} = 0$ wird, muss $P^2_n = D = a^2$, also $P_n = \pm a$ sein. Diese letzten Grössen $Q_n = 0$ und $P_n = \pm a$ entstehen, indem man den durch den gewöhnlichen Verlauf der Rechnung sich ergebenden Ausdruck

$$x_n = \frac{Q_{n-1}}{\sqrt{a^2} \mp a} \text{ in die Form } \frac{\sqrt{a^2} \pm a}{\frac{a^2 - a^2}{Q_{n-1}}} = \frac{\sqrt{a^2} \pm a}{0}$$

bringt. Hieraus leuchtet ein, dass wenn P_n nicht $= + a$, sondern $= - a$ ist,

$$x_n = \frac{Q_{n-1}}{\sqrt{a^2} + a} = \frac{\sqrt{a^2} - a}{0} = \frac{0}{0}$$

keineswegs $= \infty$ ist, sondern den bestimmten endlichen Werth

$$(1) \qquad x_n = \frac{Q_{n-1}}{\sqrt{a^2} + a} = \frac{Q_{n-1}}{2a}$$

hat.

Demnach ist, wenn sich $P_n = -a$, $Q_n = 0$ ergibt, der Schluss der Entwickelung durchaus nicht erreicht, indem nur scheinbar eine Unbestimmtheit vorliegt, auch der Quotient a_n durchaus nicht unendlich gross, sondern gleich dem grössten Subquotienten des rationalen Bruches $\frac{Q_{n-1}}{2a}$ ist. Nachdem man also den Quotienten a_n aus dem Bruche $\frac{Q_{n-1}}{2a}$ bestimmt hat, rechnet man, um bei dem nächsten Zeiger $n+1$ wieder auf die Form $\frac{\sqrt{D}+P_{n+1}}{Q_{n+1}}$ zu kommen, so weiter, dass man

$$(2) \qquad x_n = \frac{\sqrt{a^2}-a}{0} = \frac{Q_{n-1}}{2a} = a_n + \frac{1}{x_{n+1}}$$

$$(3) \qquad x_{n+1} = \frac{2a}{Q_{n-1}-2aa_n} = \frac{\sqrt{a^2}+a}{Q_{n-1}-2aa_n}$$

setzt. Demnach ist für diesen folgenden Zeiger

$$(4) \qquad P_{n+1} = a \qquad Q_{n+1} = Q_{n-1} - 2aa_n$$

und damit ist nicht allein für den Quotienten a_n, sondern auch für die Grösse Q_{n+1}, welche sich nach der Grundformel (4) des §. 61 in der vieldeutigen Form $\frac{D-P^2_{n+1}}{Q_n} = \frac{a^2-a^2}{0} = \frac{0}{0}$ darstellen würde, alle Unbestimmtheit verschwunden. Diese letztere Unbestimmtheit würde aber auch dadurch sofort vermieden sein, wenn man Q_{n+1} nicht nach Gl. (4), sondern nach Gl. (6) des §. 61 bestimmte, welche nur den vorstehenden bestimmten Werth von Q_{n+1} liefert.

Würde $Q_{n+1} = 0$ also $Q_{n-1} = 2aa_n$; so wäre bei dem Zeiger $n+1$ der Schluss der Entwickelung erreicht. Im entgegengesetzten Falle setzt man die Rechnung in bekannter Weise fort, indem man jedesmal, sowie x_n in der Form $\frac{0}{0}$ auftritt, nach der vorstehenden Regel verfährt. Endlich wird einmal in allen Fällen der durch $P_n = a$, $Q_n = 0$ sich charakterisirende wahre Schluss erreicht werden, welchen man auch daran erkennt, dass im vorhergehenden Werthe $x_{n-1} = \frac{\sqrt{a^2}+P_{n-1}}{Q_{n-1}} = \frac{a+P_{n-1}}{Q_{n-1}}$ der Nenner Q_{n-1} in dem Zähler $a+P_{n-1}$ vollständig aufgeht.

Wäre z. B. $K = \frac{\sqrt{1}+10}{9}$ gegeben, wofür man $D = 1^2$, $a = 1$, $Q_{-1} = \frac{1-10^2}{9} = -11$ hat; so ist

$$x_0 = \frac{\sqrt{1}+10}{9} = 1 + \frac{1}{x_1}$$

$$x_1 = \frac{9}{\sqrt{1}+1} = \frac{9(\sqrt{1}-1)}{0} = \frac{\sqrt{1}-1}{0}$$

$$= \frac{9}{2} = 4 + \frac{1}{x_2}$$

$$x_2 = \frac{2}{9-8} = \frac{\sqrt{1}+1}{1} = 2 + \frac{1}{x_3}$$

$$x_3 = \frac{1}{\sqrt{1}-1} = \frac{\sqrt{1}+1}{0}$$

$$\text{also } \frac{\sqrt{1}+10}{9} = \frac{11}{9} = [1, 4, 2]$$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-11		1	0
0	10	9	1	1	1
1	-1	0	4	5	4
2	1	1	2	11	9
3	1	0			

III. Es ist klar, dass man hier ebenso wie bei den irrationalen Werthen von K für die Quotienten a_n willkürliche Zahlen einführen kann, auch dass sich hier nach dem Prinzipe des §. 69 eine zweigliedrige Periode erzielen lässt, für welche die dortigen Beziehungen vollständig Gültigkeit haben, wenn man nur bei §. 69, VI. beachtet, dass möglicherweise $P_{n+1} = 0$, also Q_n oder $Q_{n+1} \leqq \sqrt{D}$ werden kann.

Die willkürlichen Quotienten, sowie die Grössen P, Q, M, N, werden stets den Grundformeln des §. 61 und 68 entsprechen, auch gelten davon die Gesetze der §§. 71, 72, 73, 74, jedoch immer mit Ausschluss der auf die Periodizität sich beziehenden Gesetze. Namentlich lassen sich auch hier zwei Entwickelungen K und K' mit derselben Determinante a^2 nach §. 73 kombiniren, wenn

$$P_m = P'_n,\ Q_m = Q'_n,\ Q_{m-1} = Q'_{n-1}$$

ist. Wir machen aber ausdrücklich darauf aufmerksam, dass wenn früher die beiden Gleichheiten $P_m = P'_n$ und $Q_m = Q'_n$ die dritte Gleichheit $Q_{m-1} = Q'_{n-1}$ nothwendig nach sich zogen, gegenwärtig eine solche Nothwendigkeit nur dann vorliegt, wenn nicht $Q_m = Q'_n = 0$ ist, also namentlich dann nicht, wenn es sich um den Schluss der Entwickelungen von K und K' handelt. Bei einem solchen Schlusse ist immer $P_m = P'_n = a$ und $Q_m = Q'_n = 0$; es können jedoch Q_{m-1} und Q'_{n-1} verschiedene Werthe haben. Die Thunlichkeit einer Kombination von K und K' am Schlusse beider Entwickelungen

setzt also nothwendig die Gleichheit der vorletzten Grössen Q_{m-1} und Q'_{n-1} voraus, und demnach werden wir im Folgenden unter den Grössen, welche der Schluss der Entwickelung von K bilden, stets die drei Grössen P_n, Q_n, Q_{n-1} verstehen.

§. 88. *Vielfachheit des Schlusses der vorstehenden Entwickelung.*

1. Es ist schon bemerkt, dass man in die Entwickelung von K auch willkürliche Quotienten einführen kann. Demnach ist man im Stande, die Entwickelung von K mittelst willkürlicher Quotienten noch über den nach vorstehendem Paragraphen erzielten Schluss fortzusetzen. Für diesen Schluss hat man bekanntlich $P_n = a$, $Q_n = 0$ also $x_n = \frac{\sqrt{a^2}+a}{0}$. Nimmt man jetzt für den Quotienten vom Zeiger n einen willkürlichen Werth a_n an; so erfordert der Übergang auf das Glied x_{n+1} eine ähnliche Aufmerksamkeit, wie der Übergang von der im vorstehenden Paragraphen sub (1) und (2) betrachteten Form $x_n = \frac{\sqrt{a_2}-a}{0}$ auf das nächste Glied x_{n+1}, damit man für die Grösse Q_{n+1}, welche sich nach §. 61 Gl. (4) in der vieldeutigen Form $\frac{0}{0}$ darstellen würde, den wahren und einzig zulässigen Werth erhalte.

Es kommt uns nämlich darauf an, dass die Grössen a_n, P_n, Q_n nicht allein den Formeln (1), (2), (3), (4), sondern auch den Formeln (5), (6) in §. 61 genügen, weil man dann erst versichert sein kann, dass dieselben auch die wichtigen Gleichungen (1), (2), (3), (4) in §. 68 erfüllen.

Nehmen wir nun für den Quotienten a_n in dem Gliede

$$(1) \qquad x_n = \frac{\sqrt{a^2}+a}{0} = a_n + \frac{1}{x_{n+1}}$$

eine beliebige ganze Zahl an; so wird nach §. 61 Gl. (2) stets $P_{n+1} = a_n Q_n - P_n = a_n . 0 - a = -a$ sein. Was aber die Grösse Q_{n+1} betrifft; so ist dieselbe, wenn sie nur die dortige Gl. (4) erfüllen soll, $= \frac{D-P_{n+1}^2}{Q_n} = \frac{a^2-a^2}{0} = \frac{0}{0}$ völlig unbestimmt. Soll dieselbe aber auch die dortige Gl. (6) erfüllen; so hat man dafür nur den einzigen bestimmten Werth

$$(2) \qquad Q_{n+1} = Q_{n-1} + 2a_n P_n - a_n^2 Q_n = Q_{n-1} + 2aa_n$$

Hiernach ist also

$$(3) \qquad x_{n+1} = \frac{\sqrt{a^2}-a}{Q_{n-1}+2aa_n}$$

Dieser Fall und der im vorhergehenden Paragraphen betrachtete, in welchem Letzteren jedoch a_n nicht willkürlich ist, sind beide durch das nachfolgende Schema dargestellt

n	P_n	Q_n	a_n
$n-1$		Q_{n-1}	
n	$\pm a$	0	a_n
$n+1$	$\mp a$	$Q_{n-1} \pm 2aa_n$	

worin sich die oberen Zeichen auf den gegenwärtigen, und die unteren Zeichen auf den früheren Fall beziehen.

II. Es ist nun beachtenswerth, dass der gegenwärtige Fall, bei welchem man einen bereits erreichten wahren Schluss von K wiederum aufgibt, um vermittelst der eingeführten willkürlichen Zahl a_n eine fernere Entwickelung mit endlichen Grössen anzubahnen, sofort zu einem neuen Schlusse gebracht werden kann, welcher mit dem früheren nicht übereinstimmt.

Einmal gelangt man zu dem neuen Schlusse, indem man den Quotienten $a_{n+1} = 0$ setzt.

Ein anderes Mal dagegen gelangt man zu dem neuen Schlusse, indem man $a_{n+1} = 1$, $a_{n+2} = -1$ setzt.

Wenngleich man noch auf unendlich verschiedene andere Weisen zu dem neuen Schlusse gelangen könnte; so umfassen doch die Werthe, welche man durch diese beiden einfachen Substitutionen zu erzielen im Stande ist, alle möglichen Schlüsse der Entwickelung von K. Die nach diesen beiden Substitutionen entstehenden Grössen sind, wie sich leicht ergibt, die folgenden:

erste Entwickelung ohne Zeichenwechsel

$a_n,\ a_{n+1} = a_n,\ 0$

n	P_n	Q_n	a_n
$n-1$		Q_{n-1}	
n	a	0	a_n
$n+1$	$-a$	$Q_{n-1}+2aa_n$	0
$n+2$	a	0	

zweite Entwickelung mit Zeichenwechsel

$a_n,\ a_{n+1},\ a_{n+2} = a_n,\ 1,\ -1$

n	P_n	Q_n	a_0
$n-1$		Q_{n-1}	
n	a	0	a_n
$n+1$	$-a$	$Q_{n-1}+2aa_n$	1
$n+2$	$Q_{n-1}+a(2a_n+1)$	$-[Q_{n-1}+2a(a_n+1)]$	-1
$n+3$	a	0	

III. Die wichtigste der durch diese Entwickelungen entstandenen Grössen ist der vorletzte Werth von Q. Derselbe ist bei der ersten Entwickelung

(4) $$Q_{n+1} = Q_{n-1} + 2aa_n$$

und bei der zweiten Entwickelung

(5) $$Q_{n+2} = -[Q_{n-1} + 2a(a_n+1)]$$

Da in beiden Werthen a_n eine beliebige positive oder ne-

gative ganze Zahl bedeutet; so sieht man, dass es möglich ist, statt des ursprünglichen Schlusses einen anderen zu erzeugen, in welchem sich der Werth des vorletzten Q von dem früheren Werthe Q_{n-1} des vorletzten Q nur durch ein Vielfaches von $2a$ unterscheidet, während gleichzeitig auch ein Zeichenwechsel eintreten kann.

Die Gesammtzahl der Glieder der ersten Entwickelung, in welcher kein Zeichenwechsel stattfindet, unterscheidet sich von der Gesammtzahl der Glieder der zweiten Entwickelung, in welcher der Zeichenwechsel vorkommt, durch eine unpaare Menge von Gliedern (hier durch ein einziges Glied).

IV. Wir behaupten nun, dass es nicht möglich ist, durch irgend welche Quotienten a_n, a_{n+1}, $a_{n+2} \dots a_{n+r}$ einen anderen Schluss, als durch die vorstehenden beiden Entwickelungen zu erzeugen.

Denn es ist klar, dass man die Fortsetzung der Entwickelung der Grösse K von der Stelle $x_n = \frac{\sqrt{D} + P_n}{Q_n}$ an vermittelst der Quotienten a_n, $a_{n+1} \dots a_{n+r}$ wie die Entwickelung einer ursprünglichen Grösse von der Form $x_0 = \frac{\sqrt{D} + P_0}{Q_0}$ auffassen kann. Alsdann hat man aber, wenn der Kettenbruch

(6) $$[a_n, a_{n+1} \dots a_{n+r}] = \frac{\mathfrak{M}_r}{\mathfrak{N}_r} \text{ und}$$

(7) $$[a_n, a_{n+1} \dots a_{n+r-1}] = \frac{\mathfrak{M}_{r-1}}{\mathfrak{N}_{r-1}}$$

gesetzt wird, nach §. 68 Gl. (1) und (2)

(8) $$\begin{cases} (-1)^{r-1} P_{n+r} = \mathfrak{M}_{r-1}\mathfrak{M}_{r-2} Q_n - (\mathfrak{M}_{r-1}\mathfrak{N}_{r-2} + \mathfrak{M}_{r-2}\mathfrak{N}_{r-1}) P_n \\ \qquad - \mathfrak{N}_{r-1}\mathfrak{N}_{r-2} Q_{n-1} \end{cases}$$

(9) $$(-1)^r Q_{n+r} = \mathfrak{M}_{r-1}^2 Q_n - 2\mathfrak{M}_{r-1}\mathfrak{N}_{r-1} P_n - \mathfrak{N}_{r-1}^2 Q_{n-1}$$

und da hier $P_n = a$, $Q_n = 0$ sein soll,

(10) $$(-1)^r P_{n+r} = (\mathfrak{M}_{r-1}\mathfrak{N}_{r-2} + \mathfrak{M}_{r-2}\mathfrak{N}_{r-1})\, a + \mathfrak{N}_{r-1}\mathfrak{N}_{r-2} Q_{n-1})$$

(11) $$(-1)^{r-1} Q_{n+r} = \mathfrak{N}_{r-1} (2a\mathfrak{M}_{r-1} + \mathfrak{N}_{r-1} Q_{n-1})$$

Addirt man zu Gl. (10) die identische Gleichung
$(-1)^r a = (\mathfrak{M}_{r-1}\mathfrak{N}_{r-2} - \mathfrak{M}_{r-2}\mathfrak{N}_{r-1})a$; so nimmt dieselbe die Form

(12) $$(-1)^r (a + P_{n+r}) = \mathfrak{N}_{r-2} (2a\mathfrak{M}_{r-1} + \mathfrak{N}_{r-1} Q_{n-1})$$

an. In diesen Gleichungen (11), (12) kann man sich unter $n+r$ einen beliebigen, also auch den vorletzten Zeiger der Entwickelung von K vorstellen. Alsdann hat man für den nächstfolgenden, also letzten Zeiger $n+r+1$, indem man $r+1$ an die Stelle von r setzt, und beachtet, dass für den nunmehr eintretenden Schluss der Entwickelung $P_{n+r+1} = a$ und $Q_{n+r+1} = 0$ sein muss, resp. nach Gl. (12) und (11)

(13) $$(-1)^{r+1}\ 2a = \mathfrak{N}_{r-1} (2a\mathfrak{M}_r + \mathfrak{N}_r Q_{n-1})$$

(14) $$0 = \mathfrak{N}_r (2a\mathfrak{M}_r + \mathfrak{N}_r Q_{n-1})$$

Da die linke Seite der Gl. (13) nicht gleich null sein kann; so ist die Gl. (14) offenbar nur durch die Bedingung

(15) $\mathfrak{N}_r = 0$

zu erfüllen. Dies führt aber wegen Gl. (13) ferner zu der Bedingung $(-1)^{r+1}\, 2a = 2a\, \mathfrak{M}_r\, \mathfrak{N}_{r-1}$ oder

(16) $\mathfrak{M}_r\, \mathfrak{N}_{r-1} = (-1)^{r+1}$

Die letzte Gleichung zerfällt aber, da $\mathfrak{M}_r$ und $\mathfrak{N}_{r-1}$ ganze Zahlen sein müssen, in folgende zwei

(17) $\mathfrak{M}_r = (-1)^s \qquad \mathfrak{N}_{r-1} = (-1)^{r+s+1}$

worin s willkürlich bleibt.

Durch den letzteren Werth von $\mathfrak{N}_{r-1}$ nimmt aber die vorletzte Grösse Q_{n+r} nach Gl. (11) den Werth

(18) $Q_{n+r} = (-1)^{r-1}\, [Q_{n-1} + (-1)^{r+s+1}\, 2a\, \mathfrak{M}'_{r-1}]$

an, welcher den obigen beiden Formen genau entspricht. Derselbe lehrt auch, dass wenn die Zahl der angehängten Quotienten a_n, $a_{n+1} \ldots a_{n+r}$, also auch $r-1$ paar ist, kein Zeichenwechsel in dem vorhin angedeuteten Sinne eintritt, dass Dies aber geschieht, wenn jene Anzahl oder $r-1$ unpaar ist. Endlich ist klar, dass die Werthe des Zählers und Nenners M_{n+r} und N_{n+r} des vorletzten Näherungsbruches, welche in die rechte Seite der Gl. (2) des §. 68 eintreten, wenn auf der linken Seite $Q_{n+r+1} = 0$ wird, für jeden beliebigen neuen Schluss entweder durch die erste oder durch die zweite der vorhin bezeichneten einfachen Entwickelungen hervorgebracht werden können, wenn man darin den Werth des Quotienten a_n angemessen bestimmt.

§. 89. *Bedingungen, unter welchen zwei Entwickelungen mit derselben quadratischen Determinante auf Ein und denselben Schluss gebracht werden können.*

I. Für zwei Entwickelungen K und K' mit derselben quadratischen Determinante a^2 sei der Schluss resp.

(1) $P_m = a,\ Q_m = 0,\ Q_{m-1}$

(2) $P'_n = a,\ Q'_n = 0,\ Q'_{n-1}$

Es fragt sich, ob und unter welchen Umständen es möglich ist, beide Entwickelungen zu Ein und demselben Schlusse zu führen, so also, dass die Werthe der vorletzten Q in beiden gleich werden.

Aus dem vorhergehenden Paragraphen Gl. (4) und (5) folgt, dass wenn a_m und a'_n zwei beliebige positive oder negative ganze Zahlen sind, mit welchen man resp. die Entwickelung von K und K' fortsetzt, in dem neuen Schlusse von K und K' der vorletzte Werth von Q resp.

(3) $Q = (Q_{m-1} + 2a\, a_m)$ oder $= -[Q_{m-1} + 2a\, (a_m + 1)]$

(4) $Q' = (Q'_{n-1} + 2a\, a'_n)$ oder $= -[Q'_{n-1} + 2a\, (a'_n + 1)]$

wird, jenachdem man die Fortsetzung nach der Entwickelung ohne oder mit Zeichenwechsel bildet.

Soll nun $Q = Q'$ sein; so muss irgend Einer der beiden Werthe von Q gleich irgend Einem der beiden Werthe von Q' gesetzt werden, um daraus die Werthe der noch unbekannten Zahlen a_m und a'_n zu bestimmen. Man findet, dass sich hierdurch nur zwei verschiedene Fälle ergeben, nämlich erstens, wenn in keiner oder wenn in beiden Fortsetzungen der Entwickelungen von K und K' ein Zeichenwechsel angenommen wird. Dies gibt

$$(5)\quad Q_{m-1} - Q'_{n-1} = 2a\,(a'_n - a_m) \text{ also } a'_n - a_m = \frac{Q_{m-1} - Q'_{n-1}}{2a}.$$

Zweitens, wenn in Einer jener beiden Entwickelungen ein Zeichenwechsel eintritt, in der anderen aber nicht. Dies gibt

$$(6)\quad \begin{cases} Q_{m-1} + Q'_{n-1} = -2a\,(a'_n + a_m + 1) \text{ also} \\ a'_n + a_m \quad = -\left(\dfrac{Q_{m-1} + Q'_{n-1}}{2a} + 1\right) \end{cases}$$

Die Möglichkeit, K und K' zu demselben Schlusse zu führen, liegt also nur dann vor, wenn entweder die Differenz oder die Summe von Q_{m-1} und Q'_{n-1} eine durch $2a$ theilbare (also jedenfalls paare) Zahl ist. Im ersten Falle ist a_m und a'_n nach Gl. (5), im zweiten Falle nach Gl. (6) zu bestimmen.

Da hiernach Eine der beiden Zahlen a_m und a'_n willkürlich bleiben würde; so ist es das Einfachste, nicht beide Entwickelungen K und K', sondern nur die Eine davon fortzusetzen und auf den Schluss der anderen zu bringen.

II. Nehmen wir also an, es solle blos K' fortgesetzt und mit K in Übereinstimmung gebracht werden. Dies kann geschehen erstens, wenn die Differenz $Q_{m-1} - Q'_{n-1}$ durch $2a$ theilbar ist, indem man K' nach der ersten Entwickelungsweise des vorhergehenden Paragraphen ohne Zeichenwechsel, also für $a'_n,\ a'_{n+1} = a'_n,\ 0$ fortsetzt und

$$(7)\qquad a'_n = \frac{Q_{m-1} - Q'_{n-1}}{2a}$$

nimmt. Zweitens, wenn die Summe $Q_{m-1} + Q'_{n-1}$ durch $2a$ theilbar ist, indem man K' nach der zweiten Entwickelungsweise des vorhergehenden Paragraphen mit Zeichenwechsel, also für $a'_n,\ a'_{n+1},\ a'_{n+2} = a'_n,\ 1,\ -1$ fortsetzt und

$$(8)\qquad a'_n = -\left(\frac{Q_{m-1} + Q'_{n-1}}{2a} + 1\right)$$

nimmt.

Für den speziellen Fall, wo $Q'_{n-1} = -Q_{m-1}$ sein sollte, ist die Summe $Q_{m-1} + Q'_{n-1} = 0$ stets durch $2a$ theilbar. Man kann also von dem Schlusse $a,\ 0,\ Q'_{n-1}$ stets auf den Schluss $a,\ 0,\ -Q'_{n-1}$ gelangen, wenn man nach Gl. (8) verfährt, also $a'_n,\ a'_{n+1},\ a'_{n+2} = -1,\ 1,\ -1$ setzt.

Beispiel 1. Für die Determinante $36 = 6^2$ also $a = 6$ habe man

	in K			in K'	
m	P_m	Q_m	n	P'_n	Q'_n
$m-1$		13	$n-1$		1
m	6	0	n	6	0

Da hier die Differenz $Q_{m-1} - Q'_{n-1} = 13 - 1 = 12$ durch $2a = 12$ theilbar ist; so kann K' zu dem Schlusse von K gebracht werden, indem man nach Gl. (7) $a'_n = \frac{13-1}{2.6} = 1$, $a'_{n+1} = 0$ setzt. Dies gibt für die Fortsetzung von K'

n	P'_n	Q'_n	a'_n
$n-1$		1	
n	6	0	1
$n+1$	-6	13	0
$n+2$	6	0	

Beispiel 2. Für dieselbe Determinante habe man

	in K			in K'	
m	P_m	Q_m	n	P'_n	Q'_n
$m-1$		7	$n-1$		5
m	6	0	n	6	0

Da hier die Summe $Q_{m-1} + Q'_{n-1} = 7 + 5 = 12$ durch $2a = 12$ theilbar ist; so kann K' zu dem Schlusse von K gebracht werden, indem man nach Gl. (8) $a'_n = -\left(\frac{7+5}{2.6} + 1\right) = -2$, $a'_{n+1} = 1$, $a'_{n+2} = -1$ setzt. Dies gibt als Fortsetzung von K'

n	P'_n	Q'_n	a'_n
$n-1$		5	
n	6	0	-2
$n+1$	-6	-19	1
$n+2$	-13	7	-1
$n+3$	6	0	

Beispiel 3. Wäre im vorstehenden Beispiele $Q'_{n-1} = -7$; so kann, da die Summe $Q_{m-1} + Q'_{n-1} = 7 + (-7) = 0$ durch $2a$ theilbar ist, K' zu dem Schlusse von K gebracht werden, indem man nach Gl. (8) $a'_n = -1$, $a'_{n+1} = 1$, $a'_{n+2} = -1$ setzt. Dies gibt als Fortsetzung von K'

n	P'_n	Q'_n	a'_n
$n-1$		-7	
n	6	0	-1
$n+1$	-6	-19	1
$n+2$	-13	7	-1
$n+3$	6	0	

§. 90. Schluss in kleinsten positiven Zahlen.

I. Da sich die Werthe der vorletzten Grössen Q in allen möglichen Schlüssen von K nur durch ein Vielfaches von $2a$ und durch das Zeichen unterscheiden; so ist klar, dass man stets einen Schluss herstellen kann, in welchem das vorletzte Q positiv und $\leqq a$ ist, auch dass es nur ein einziges Q dieser Art geben kann.

Um diesen Schluss, welchen wir den Schluss in kleinsten positiven Zahlen nennen wollen, zu erreichen; so sei Q_{n-1} der Werth des vorletzten Q in irgend einem bereits dargestellten Schlusse. Dividirt man mit $2a$ in Q_{n-1}; so sei w der grösste Subquotient, insofern der entstehende positive Rest $R \leqq a$ ist, sodass man dann

(1) $$Q_{n-1} = 2aw + R \text{ und } R = Q_{n-1} - 2aw$$

hat. Dagegen sei w der kleinste Superquotient, insofern für den hierdurch entstehenden negativen Rest $-R$ der absolute Betrag $R \leqq a$ ist, sodass man dann

(2) $$Q_{n-1} = 2aw - R \text{ und } R = -(Q_{n-1} - 2aw)$$

hat.

Vergleicht man hiermit resp. die Gl. (4) und (5) in §. 88; so leuchtet ein, dass man den Schluss in kleinsten positiven Zahlen erhält, wenn man im ersten Falle

(3) $$a_n = -w, \quad a_{n+1} = 0$$

und im zweiten Falle

(4) $$a_n = -(w+1), \quad a_{n+1} = 1, \quad a_{n+2} = -1$$

setzt. In beiden Fällen wird für den neuen Schluss das vorletzte $Q = R$.

Stellt man also in den beiden Entwickelungen K und K', welche dieselbe Determinante haben, die Schlüsse in kleinsten positiven Zahlen her, für welche das vorletzte Q positiv und $\leqq a$ sein muss; so müssen diese Werthe von Q aus K und K' identisch sein, wenn es möglich sein soll, K und K' miteinander zu kombiniren, weil im entgegengesetzten Falle K und K' auf keine Weise zu übereinstimmenden Schlüssen gebracht werden können.

Der Umstand, dass in dem neuen Schlusse das vorletzte Q den Werth des betreffenden Restes R annimmt, liefert zugleich das einfachste Mittel, die möglichen Übereinstimmungen mehrerer Entwickelungen miteinander zu vergleichen.

So ist z. B. in dem ersten Beispiele des vorhergehenden Paragraphen der Schluss von K' Einer in kleinsten positiven Zahlen, weil darin das vorletzte $Q = 1$ positiv und $< a$, nämlich < 6 ist. Der Schluss von K, worin jenes $Q = 13$ ist, besitzt diese Eigenschaft nicht. Will man ihn dahin bringen; so hat man, da $2a = 12$ ist, $13 = 12.1 + 1$. Es ist also $R = 1$,

$w = 1$ und nach Gl. (3) $a_n = -1$, $a_{n+1} = 0$ zu setzen, um auch K zu dem Schlusse 6, 0, 1 zu bringen.

In dem zweiten Beispiele des vorhergehenden Paragraphen ist der Schluss von K' Einer in kleinsten positiven Zahlen, weil darin das vorletzte $Q = 5$ positiv und < 6 ist. Da dieses Minimum 5 mit dem vorhergehenden Minimum 1 nicht übereinstimmt; so folgt, dass die Entwickelungen von K' aus dem ersten und von K' aus dem zweiten Beispiele nicht zu einem übereinstimmenden Schlusse gebracht werden können. Wol aber ist Dies mit dem letzteren K' und dem K aus dem zweiten Beispiele möglich, wofür $Q_{n-1} = 7$ ist. Um diesen Schluss von K ebenfalls auf kleinste positive Zahlen zu bringen, hat man, da $2a = 12$ ist, $7 = 12.1 - 5$. Es ist also $R = 5$, $w = 1$ und nach Gl. (4) $a_n = -2$, $a_{n+1} = 1$, $a_{n+2} = -1$ zu setzen, um den Schluss 6, 0, 5 zu erlangen.

II. Wir bemerken noch, dass die meisten Entwickelungen K mit grössten Subquotienten von selbst zu dem Schlusse mit kleinsten positiven Zahlen führen. Mit Ausnahme derjenigen nämlich, wo der Schluss schon in den obersten Zeigern erreicht wird, gelangt man stets an eine Stelle, von wo an alle folgenden P positiv und $\leqq a$ und alle folgenden Q positiv sind. Ist nun jenseit dieser Stelle $x_{n-1} = \frac{\sqrt{a^2} + P_{n-1}}{Q_{n-1}}$ das dem Schlusse unmittelbar vorhergehende Glied; so muss bekanntlich Q_{n-1} in $\sqrt{a^2} + P_{n-1} = a + P_{n-1} \leqq 2a$ aufgehen oder ein Faktor davon sein. Es ist aber nicht möglich, dass $Q_{n-1} = a + P_{n-1}$ also $x_{n-1} = 1$ und demnach $a_{n-1} = 1$ sei, weil die Entwickelung eines rationalen Bruches K mit grössten Subquotienten niemals als letzten Quotienten den Werth 1 ergeben kann (§. 10.) Wenn aber Q_{n-1} nicht $= 2a$ sein kann; so muss es $\leqq a$ sein, also einem Schlusse mit kleinsten positiven Zahlen angehören.

III. Es ist noch von Wichtigkeit, zu untersuchen, unter welchen Umständen es möglich ist, dass die Werthe von R in den beiden Formeln (1) und (2) einander gleich seien, also ebenso gut die Formel (1), wie die Formel (2) angewendet werden kann.

Bezeichnet man zu diesem Ende das w in Gl. (2), zum Unterschiede von dieser Grösse in Gl. (1) mit w'; so muss sein

$$Q_{n-1} = 2aw + R = 2aw' - R$$

Diese Beziehung ist in zwei Fällen möglich, erstens, wenn Q_{n-1} ein paares Vielfaches von a oder ein Vielfaches von $2a$ ist, indem man dann $R = 0$ und $w = w' = \frac{Q_{n-1}}{2a}$ hat. Dieser Fall tritt immer ein, wenn $Q_{n-1} = 0$ ist, also bei dem Schlusse a, 0, 0.

Zweitens, wenn Q_{n-1} ein unpaares Vielfaches von a ist, indem dann $R = a$ und $w' = w + 1$ ist. Dieser Fall tritt z. B. ein für $a = 1$, wenn gleichzeitig $Q_{n-1} = 1$, also der Fluss 1, 0, 1 ist.

In diesen beiden Fällen, in welchen Q_{n-1} irgend ein Vielfaches von a ist, kann man also den Schluss in kleinsten positiven Zahlen sowol nach der Formel (3), wie auch nach (4) erzeugen, oder wenn er schon erzeugt ist, nochmals reproduziren. Die Zeiger für die letzten Glieder der hieraus nach (3) oder (4) hervorgehenden Schlüsse unterscheiden sich dann durch eine unpaare Differenz, und hierin besteht eine gewisse Zweideutigkeit, welche in diesen Fällen dem Schlusse in kleinsten positiven Zahlen anhaftet.

§. 91. *Entwickelung von* $K = \frac{\sqrt{a^2} \pm a}{0}$.

I. Wenn in dem zu entwickelnden Ausdrucke $K = \frac{\sqrt{a^2} + P_0}{Q_0}$ der Nenner $Q_0 = 0$ ist; so eignet sich dieser Ausdruck nur dann zu unserer Betrachtung, wenn $P_0 = \pm a$ ist. Hätte P_0 einen anderen Werth; so würde $Q_{-1} = \frac{a^2 - P_0^2}{Q_0} = \infty$ werden, ein Fall, der für uns kein Interesse hat.

Wenn jedoch $P_0 = \pm a$ ist; so wird $Q_{-1} = \frac{a^2 - a^2}{0} = \frac{0}{0}$ und kann sehr wohl endliche Werthe haben. Man muss nun unterscheiden, ob durch irgend eine besondere Bedingung der Werth von Q_{-1} als ein völlig bestimmter gegeben ist, oder ob für die Grösse Q_{-1} keine Bedingungsgleichung gegeben, diese Grösse also willkürlich ist. Beide Umstände können bei den diophantischen Gleichungen vom zweiten Grade eintreten: der erste, wenn nach §. 74 die Grössen D, P_0, Q_0, Q_{-1} aus den Koeffizienten einer gegebenen Gleichung abgeleitet werden; der zweite, wenn man nach demselben Paragraphen den dortigen Ausdruck (6) herstellt, worin q gegeben und p gefunden, aber r an keine spezielle Bedingung geknüpft ist.

II. Ist nun $P_0 = +a$; so stellt $P_0, Q_0, Q_{-1} = a, 0, Q_{-1}$ bereits den Schluss der Entwickelung dar. Derselbe ist ein einziger, wenn Q_{-1} bestimmt ist. Wäre jedoch Q_{-1} willkürlich; so würde es unendlich viele verschiedene Schlüsse geben. Hiervon sind jedoch nach vorhergehendem Paragraphen nur diejenigen mit kleinsten positiven Zahlen von Wichtigkeit. Die letzteren erhält man sämmtlich, wenn man für Q_{-1} nach und nach Eine der $(a + 1)$ Zahlen 0, 1, 2, 3 ... a setzt.

III. Ist aber $P_0 = -a$; so stellt $P_0, Q_0, Q_{-1} = -a, 0, Q_{-1}$

den Schluss nicht dar. Wäre nun Q_{-1} bestimmt; so ist es leicht, den gegebenen Ausdruck in der nur einzig möglichen Weise zum Schlusse zu führen. Man hat nämlich nach §. 87 Gl. (1) und (2) den Ausdruck

$$(1) \qquad x_0 = \frac{\sqrt{a^2} - a}{0} = \frac{Q_{-1}}{2a} = a_0 + \frac{1}{x_1}$$

zu setzen, worin a_0 der grösste Subquotient des vollkommen bestimmten Bruches $\frac{Q_{-1}}{2a}$ ist. Dies gibt dann ferner

$$(2) \qquad x_1 = \frac{2a}{Q_{-1} - 2aa_0} = \frac{\sqrt{a^2} + a}{Q_{-1} - 2aa_0} = a_1 + \frac{1}{x_2}$$

womit man in bekannter Weise weiterrechnet.

Wäre dagegen Q_{-1} willkürlich; so würde man den ersten Quotienten a_0 aus den unendlich verschiedenen Brüchen $\ldots \frac{-2}{2a}, \frac{-1}{2a}, \frac{0}{2a}, \frac{1}{2a}, \frac{2}{2a} \ldots$ bestimmen müssen. Dies gibt ebenso viel verschiedene Entwickelungen. Die Anzahl der daraus hervorgehenden verschiedenen Schlüsse mit kleinsten positiven Zahlen ist jedoch keineswegs unendlich gross, sondern wie in dem vorhergehenden Falle, wo $P_0 = a$ war, $= a + 1$, und man erhält dieselben, wenn man für Q_{-1} nach und nach die Zahlen 0, 1, 2, 3 ... a nimmt.

Denn nach Gl. (2) ist stets, welches auch der Werth des Quotienten a_0 sei, für den nächsten Zeiger $P_1 = a$ und $Q_1 = Q_{-1} - 2aa_0$. Welchen Werth nun auch Q_{-1} habe, immer kann man a_0 so wählen, dass Q_1 positiv und $\leqq a$ wird (wobei natürlich a_0 nicht immer den grössten Subquotienten des Ausdruckes (1) darstellt). Ferner ist klar, dass wenn man nach und nach $Q_{-1} = 0, 1, 2 \ldots a$ setzt, und immer a_0 so bestimmt, dass Q_1 positiv und $\leqq a$ wird, für Q_1 nach und nach jeder Werth der Zahlen 0, 1, 2 ... a, wenn auch in einer anderen Reihenfolge auftreten wird. Demnach kann es höchstens $a + 1$ verschiedene Schlüsse geben.

Es gibt aber auch nicht weniger, als $a + 1$ verschiedene Schlüsse. Dies kann durch eine Ableitung dargethan werden, welche der in §. 88 angewandten ähnlich ist. Gehen wir nämlich von den dortigen Formeln (8) und (9) aus; so haben wir, indem wir uns unter den Grössen P_n, Q_n, Q_{n-1} die jetzigen Grössen P_0, Q_0, Q_{-1} denken, also $n = 0$ setzen, $P_0 = -a$, $Q_0 = 0$ zu setzen. Dies gibt statt der dortigen Gleichungen (10) und (11)

$$(3) \quad (-1)^r \; P_r = -(\mathfrak{M}_{r-1}\mathfrak{N}_{r-2} + \mathfrak{M}_{r-2}\mathfrak{N}_{r-1})\,a + \mathfrak{N}_{r-1}\mathfrak{N}_{r-2}\,Q_{-1}$$

$$(4) \quad (-1)^{r-1} Q_r = \mathfrak{N}_{r-1}(-2a\mathfrak{M}_{r-1} + \mathfrak{N}_{r-1}\,Q_{-1})$$

und wenn man zu Gl. (3) die identische Gleichung $(-1)^r a = (\mathfrak{M}_{r-1}\mathfrak{N}_{r-2} - \mathfrak{M}_{r-2}\mathfrak{N}_{r-1})\,a$ addirt,

$$(5) \qquad (-1)^r (a + P_r) = \mathfrak{N}_{r-1}(-2a\mathfrak{M}_{r-2} + \mathfrak{N}_{r-2}\,Q_{-1})$$

Stellt man sich in Gl. (4), (5) unter r den vorletzten Zeiger, also unter $r+1$ den letzten Zeiger der Entwickelung von K vor, womit der Schluss eintritt; so muss $P_{r+1}=a$, $Q_{r+1}=0$ sein. Demnach hat man, wenn man in diesen Gleichungen r in $r+1$ übergehen lässt,

(6) $$(-1)^{r+1}2a=\mathfrak{N}_r(-2a\mathfrak{M}_{r-1}+\mathfrak{N}_{r-1}Q_{-1})$$

(7) $$0=\mathfrak{N}_r(-2a\mathfrak{M}_r+\mathfrak{N}_r\,Q_{-1})$$

Hierin darf offenbar $\mathfrak{N}_r$ nicht $=0$ gesetzt werden, was der Gl. (6) widersprechen würde. Es kann also nur

$$-2a\mathfrak{M}_r+\mathfrak{N}_rQ_{-1}=0 \text{ also}$$

(8) $$\frac{\mathfrak{M}_r}{\mathfrak{N}_r}=[a_0,\ a_1\dots a_r]=\frac{Q_{-1}}{2a}$$

sein, was auch der Gl. (1) entspricht. Aus Gl. (6) folgt

$$-2a\mathfrak{M}_{r-1}+\mathfrak{N}_{r-1}Q_{-1}=\frac{(-1)^{r+1}2a}{\mathfrak{N}_r}$$

und wenn man diesen Werth in Gl. (4) substituirt; so ergibt sich für das vorletzte Q des Schlusses

(9) $$Q_r=\frac{2a\mathfrak{N}_{r-1}}{\mathfrak{N}_r}$$

Da $\mathfrak{N}_r$ und $\mathfrak{N}_{r-1}$ stets relative Primzahlen sind (§. 13) so muss, da Q_r eine ganze Zahl ist, $\mathfrak{N}_r$ ein Faktor von $2a$ sein, was auch aus Gl. (8) erhellet. Setzt man das grösste gemeinschaftliche Maass von Q_{-1} und $2a$ gleich m; so muss wegen Gl. (8)

(10) $$Q_{-1}=m\mathfrak{M}_r \qquad 2a=m\mathfrak{N}_r \text{ oder}$$

(11) $$\mathfrak{M}_r=\frac{Q_{-1}}{m} \qquad \mathfrak{N}_r=\frac{2a}{m}$$

und demnach wegen Gl. (9)

(12) $$Q_r=m\mathfrak{N}_{r-1}$$

sein. Substituirt man nun nach und nach in Gl. (8) für $Q_{-1}=m\mathfrak{M}_r$ die Werthe 0, 1, 2 ... a; so ergeben sich lauter verschiedene Werthe für den Bruch $\frac{\mathfrak{M}_r}{\mathfrak{N}_r}=\frac{m\mathfrak{M}_r}{m\mathfrak{N}_r}$, also auch für die Quotientenreihe $[a_0,\ a_1\dots a_r]$, welche die Entwickelung jener Brüche mit grössten Subquotienten darstellen soll, und es ist zu beachten, dass in diesen verschiedenen Brüchen stets $m\mathfrak{M}_r \leqq a$ und $m\mathfrak{N}_r=2a$ ist, also jeder Bruch $\leqq \frac{1}{2}$ und demnach in allen $a_0=0$ ist.

Kehrt man die vorstehende Quotientenreihe um; so hat nach §. 13 der reduzirte Kettenbruch

$$[a_r,\ a_{r-1}\dots a_0] \text{ den Werth } \frac{\mathfrak{N}_r}{\mathfrak{N}_{r-1}}=\frac{m\mathfrak{N}_r}{m\mathfrak{N}_{r-1}}$$

und Dies gibt ebenfalls $a+1$ verschiedene Werthe, jenachdem man $Q_{-1}=0,\ 1,\ 2\dots a$ setzt. Nun ist aber in der Ent-

wickelung eines jeden echten Bruches $\frac{\mathfrak{M}_r}{\mathfrak{N}_r}$ nach §. 10 der letzte Quotient a_r stets > 1. Mithin ist der Werth von $[a_r, a_{r-1} \ldots a_0] \geqq 2$, d. i.

$$\frac{m\mathfrak{N}_r}{m\mathfrak{N}_{r-1}} = \frac{2a}{m\mathfrak{N}_{r-1}} \geqq 2 \text{ folglich}$$

(13) $$m\mathfrak{N}_{r-1} = Q_r \leqq a$$

Von dieser letzten Behauptung wäre nur der Fall ausgenommen, wo man $Q_{-1} = m\mathfrak{M}_r = 0$ setzte. Alsdann ist aber sofort

n	P_n	Q_n	a_n
-1		0	
0	$-a$	0	0
1	a	0	

also der Schluss beim Zeiger 1 erreicht und $Q_r = 0$, was für keinen anderen Werth von $Q_{-1} \leqq a$ möglich ist.

Hieraus folgt nun, dass jenachdem man $Q_{-1} = 0, 1, 2, \ldots a$ setzt, $a+1$ verschiedene Schlüsse auftreten werden, für welche in kleinsten positiven Zahlen das vorletzte Q dieselben Werthe, wenn auch in anderer Reihenfolge annimmt, dass also in diesem Falle, wo $P_0 = -a$ vorausgesetzt war, ebenso wie in dem vorhergehenden Falle, wo $P_0 = a$ vorausgesetzt war, jeder denkbare Schluss zu erreichen steht, sobald Q_{-1} willkürlich ist, und dass man, um alle verschiedenen Schlüsse in kleinsten positiven Zahlen zu erhalten, nur $Q_{-1} = 0, 1, 2 \ldots a$ zu setzen braucht.

§. 92. *Zahlenreihe, welche im Stande ist, die bei der Entwickelung der Grösse K mit quadratischer Determinante vorkommenden Operationen zu ersetzen.*

I. Es hat keine Schwierigkeit, die Resultate der §§. 75 bis 81 über die Zahlen von der Form $J_p = D - p^2$ auf den gegenwärtigen Fall zu übertragen, wo D ein vollkommenes Quadrat, also $J_p = a^2 - p^2$ ist. Es ändert sich hierdurch Nichts an den allgemeinen Resultaten. Im Speziellen jedoch bemerken wir, dass hier die Gränzlinie $\alpha\alpha$ der positiven und negativen Zahlen J durch ein Glied jener Reihe, für welches man $p = a$ also $J_a = a^2 - a^2 = 0$ hat, hindurchgeht. Dieser Werth 0, welcher jederzeit unter den Zahlen J erscheint, welches auch die quadratische Determinante a^2 sein mag, kann als das Produkt aus 0 und jeder beliebigen positiven oder negativen Zahl w angesehen werden. Daraus folgt, dass jede ganze Zahl w unter den Faktoren der Zahlen J erscheinen wird, wenn die Determinante ein Quadrat ist.

So hat man z. B. für $D = a^2 = 16$

	J_0	$16-0^2$	16	$1.2.2.2.2$
J_{-1}	J_1	$16-1^2$	15	$1.3.5$
J_{-2}	J_2	$16-2^2$	12	$1.2.2.3$
J_{-3}	J_3	$16-3^2$	7	1.7
α——J_{-4}	J_4	$16-4^2$	0	$0.w$——α
J_{-5}	J_5	$16-5^2$	-9	$-1.3.3$
J_{-6}	J_6	$16-6^2$	-20	$-1.2.2.5$
J_{-7}	J_7	$16-7^2$	-33	$-1.3.11$

u. s. w.

II. Die Kettenbruchsentwickelung hat hier das Ziel, in die Linie αα selbst, aber nicht in das Glied J_{-4}, sondern in das Glied J_4 hineinzugelangen und daselbst zu schliessen. Die Fortsetzung des Mechanismus nach §. 75 für den Fall, dass man auf den Werth $\frac{\sqrt{a^2}+a}{Q_n}$ stösst, also im Gliede J_{-4} die Zählung beginnen muss, hat keine Schwierigkeit, und wäre $Q_n=0$; so befände man sich sogar am Schlusse, welchen man übrigens mit willkürlichen Quotienten auch überschreiten kann. Wenn man jedoch auf den Werth $\frac{\sqrt{a^2}-a}{Q_n}$ stösst, also im Gliede J_4 die Zählung beginnen muss; so kann Dies zwar dann immer leicht geschehen, wenn Q_n verschieden von null ist, indem dann $a_n=0$ ist und in bekannter Weise ein Stillstand eintritt, welcher gegenwärtig sogar den Schluss herbeiführt: wenn aber $Q_n=0$ ist, also der Werth $\frac{\sqrt{a^2}-a}{0}=\frac{0}{0}$ vorliegt, und es sich um eine Entwickelung mit grössten Subquotienten handelt, wobei der nächste Quotient a_n nicht willkürlich gegeben, sondern gesucht ist; so ist zwar klar, dass durchaus ein Stillstand auf dem Gliede J_4 stattfinden muss, weil $Q_n a_n = 0.a_n$ stets $=0$ und demnach kein Heraustreten aus dem Gliede J_4 möglich ist; allein es fehlt zuvörderst an einer Bedingung für die Grösse a_n, und ausserdem fehlt es bei der Fortsetzung der Rechnung an einer Bestimmung für Q_{n+1}, welche Grösse durch Division mit $Q_n=0$ in $Q_n Q_{n+1}=0$ zu erzielen sein würde. Diese letzteren Unbestimmtheiten sind nach §. 87 zu beseitigen, indem in diesem Falle a_n der grösste Subquotient des Bruches $\frac{Q_{n-1}}{2a}$ und $Q_{n+1}=Q_{n-1}-2a\,a_n$ sein muss.

III. Die verschiedenen Reihen der durch eine gegebene Zahl q theilbaren Zahlen J erhält man durch dieselben in §. 76, 77 ff. gelehrten Methoden. Es muss auch hier für Ein Glied jeder Reihe, wenn q paar ist, $p\leqq\frac{q}{2}$, und wenn q unpaar ist, $p\leqq\frac{q-1}{2}$ sein.

So hat man z. B. für $D = 16$ und $q = 12$ die beiden Reihen

$\ldots J_{-20} \quad J_{-8} \quad J_4 \quad J_{16} \ldots = -384 \quad -48 \quad 0 \quad -240 \ldots$

$\ldots J_{-22} \quad J_{-10} \quad J_2 \quad J_{14} \ldots = -468 \quad -84 \quad 12 \quad -180 \ldots$

und die konjugirten Reihen davon.

IV. Eine Reihe der durch q theilbaren Zahlen geht stets durch das Glied $J_a = 0$, und die konjugirte Reihe durch das Glied J_{-a}. Wenn q eine Primzahl ist; so gibt es nach §. 80 nur eine einzige Reihe dieser Art (ausser der konjugirten) welche also die durch das Glied J_a gehende sein muss.

V. Im gegenwärtigen Falle kann auch $q = 0$ sein. Es gibt jedoch dann keine Reihen der durch 0 theilbaren Zahlen J, sondern nur zwei einzelne Glieder, nämlich $J_a = a^2 - a^2 = 0$ und $J_{-a} = a^2 - a^2 = 0$, auf welche sich jene Reihen gewissermaassen konzentriren.

Fall, wo die Determinante gleich null ist.

§. 93. Eigenthümlichkeiten des Falles, wo die Determinante $D = 0$ ist.

I. Dieser Fall ist eine Spezialität des vorhin betrachteten wo die Determinante ein Quadrat a^2 war. Man hat hier $a = 0$. Die Entwickelung der Grösse $K = \frac{\sqrt{0} + P_0}{Q_0}$ ist ebenso wie im vorhergehenden Falle zu bewirken. Die beiden dort besonders untersuchten Glieder $\frac{\sqrt{a^2} \pm a}{Q_n}$ fallen hier jedoch in ein einziges $\frac{\sqrt{0} + 0}{Q_n}$ zusammen, und erfordern demnach keine Unterscheidung. Der Schluss der Entwickelung ist erreicht, wenn

$$P_n,\ Q_n,\ Q_{n-1} = 0,\ 0,\ Q_{n-1}$$

also $x_n = \frac{\sqrt{0} + 0}{0}$ wird. Es wird übrigens auch hier stets vorausgesetzt, dass $Q_{-1} = \frac{D - P_0^2}{Q_0} = \frac{-P_0^2}{Q_0}$ eine ganze Zahl sei.

So hat man z. B. für $K = \frac{\sqrt{0} + 30}{45}$, worin $Q_{-1} = \frac{30^2}{45} = 20$ ist,

$$x_0 = \frac{\sqrt{0} + 30}{45} = 0 + \frac{1}{x_1}$$

$$x_1 = \frac{45}{\sqrt{0} + 30} = \frac{45(\sqrt{0} - 30)}{-900} = \frac{\sqrt{0} - 30}{-20} = 1 + \frac{1}{x_2}$$

$$x_2 = \frac{-20}{\sqrt{0} - 10} = \frac{-20(\sqrt{0} + 10)}{-100} = \frac{\sqrt{0} + 10}{5} = 2 + \frac{1}{x_3}$$

$$x_3 = \frac{5}{\sqrt{0}+0} = \frac{5(\sqrt{0}+0)}{0} = \frac{\sqrt{0}+0}{0}$$

also $K = \frac{\sqrt{0}+30}{45} = \frac{30}{45} = [0,\ 1,\ 2]$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		20		1	0
0	30	45	0	0	1
1	-30	-20	1	1	1
2	10	5	2	2	3
3	0	0			

II. Im gegenwärtigen Falle ändern sich jedoch die Resultate des §. 88, 89 und 90 über die Vielfachheit des Schlusses und über den Schluss in kleinsten positiven Zahlen.

Da hier nämlich $a = 0$ ist; so wird, nachdem der Schluss 0, 0, Q_{n-1} erreicht ist, welchen Werth man auch für den Quotienten a_n setzen möge, stets

$$Q_{n-1} + 2aa_n = Q_{n-1} \text{ und}$$
$$-[Q_{n-1} + 2a(a_n+1)] = -Q_{n-1}$$

sein. Man kann also keinen zweiten Schluss erzeugen, in welchem das vorletzte Q einen anderen absoluten Werth besässe, als in dem zuerst gefundenen Schlusse. Wol aber kann man einen neuen Schluss hervorbringen, in welchem das vorletzte Q das entgegengesetzte Zeichen des früheren hat. Es lässt sich also stets ein Schluss mit positivem vorletztem Q erzielen.

III. Aus den Formeln für die Grössen P und Q in §. 61 erkennt man, dass hier, wo $D = 0$ ist, das grösste gemeinschaftliche Maass der drei Grössen P_0, Q_0 und $Q_{-1} = -\frac{P_0^2}{Q_0}$ ein gemeinschaftlicher Faktor aller Grössen P, Q, also auch des vorletzten Q ist. Da dieses vorletzte Q, oder Q_{n-1}, offenbar in P_{n-1} enthalten, oder $P_{n-1} = a_{n-1}Q_{n-1}$ sein muss; so erkennt man auch aus jenen Formeln, indem man in der Bildung der Grössen P, Q rückwärts geht, dass jenes vorletzte Q ein gemeinschaftlicher Faktor aller Grössen P, Q sei.

Demnach erhellet, dass das vorletzte Q, also Q_{n-1}, stets das grösste gemeinschaftliche Maass der drei Grössen P_0, Q_0, Q_{-1}, dass also, wenn diese drei Grössen relativ prim sind, was in der Anwendung auf die unbestimmten Gleichungen stets vorausgesetzt werden kann, $Q_{n-1} = \pm 1$ sei. In diesem Falle kann man also immer einen Schluss in positiven Zahlen erzeugen, für welchen $Q_{n-1} = 1$ ist.

IV. Wenn w eine willkürliche Zahl bedeutet; so liefert die Substitution a_n, $a_{n+1} = w$, 0 stets genau denselben Schluss und die Substitution a_n, a_{n+1}, $a_{n+2} = w$, 1, -1 stets einen Schluss, worin das vorletzte Q nur das entgegengesetzte Zeichen

hat (§. 88). Diese beiden Entwickelungen sind durch folgendes Schema dargestellt.

erste Entwickelung ohne Zeichenwechsel				zweite Entwickelung mit Zeichenwechsel			
$a_n, a_{n+1} = w, 0$				$a_n, a_{n+1}, a_{n+2} = w, 1, -1$			
n	P_n	Q_n	a_n	n	P_n	Q_n	a_n
$n-1$		Q_{n-1}		$n-1$		Q_{n-1}	
n	0	0	w	n	0	0	w
$n+1$	0	Q_{n-1}	0	$n+1$	0	Q_{n-1}	1
$n+2$	0	0		$n+2$	Q_{n-1}	$-Q_{n-1}$	-1
				$n+3$	0	0	

V. Wäre $K = \frac{\sqrt{0}+0}{0}$ gegeben; so reduzirt sich die Betrachtung des §. 91 auf die Bemerkung, dass hierdurch immer schon ein Schluss der Entwickelung dargestellt ist. Ist nun durch eine besondere Bedingung Q_{-1} gegeben; so ist der Schluss mit positivem vorletzten Q einzig. Ist dagegen Q_{-1} willkürlich; so kann ein Schluss mit jedem beliebigen Werthe des vorletzten Q dargestellt werden. Alle diese Schlüsse kann man stets so einrichten, dass ihnen unter den Quotienten des Kettenbruchs eine willkürliche Zahl w vorhergeht.

VI. Die Reihe der Zahlen J, welche jetzt nur die negativen Werthe der sukzessiven Quadratzahlen $0, -1, -4, -9\ldots$ enthält, und bei welcher die frühere Gränzlinie $\alpha\alpha$ durch das obere Glied J_0 geht, ist wie vorhin zu gebrauchen.

VII. Auch sind in dieser Reihe die durch eine gegebene Zahl q theilbaren Zahlen nach den obigen Regeln aufzusuchen. So hat man z. B. für $q=9$ die symmetrische Reihe

$$\ldots J_{-9} \quad J_0 \quad J_9 \ldots = \ldots -81 \quad 0 \quad -81 \ldots$$

und ausserdem die Reihe

$$\ldots J_{-6} \quad J_3 \quad J_{12} \ldots = \ldots -36 \quad -9 \quad -144 \ldots$$

nebst der konjugirten davon.

VIII. Auch im gegenwärtigen Falle kann $q=0$ gegeben sein. Die durch 0 theilbaren Zahlenreihen konzentriren sich aber auf das einzige Glied $J_0=0$.

Fall, wo die Determinante negativ ist.

§. 94. *Entwickelung einer imaginären Quadratwurzel in einen Kettenbruch.*

I. In dem gegenwärtigen Falle, wo die Determinante negativ sein soll, wollen wir dieselbe mit $-D$ bezeichnen. Es ist klar, dass wenn der imaginäre Ausdruck $K = \frac{\sqrt{-D}+P_0}{Q_0}$ durch eine Kettenbruchsentwickelung erschöpft werden soll,

unter den Quotienten nothwendig imaginäre Werthe zugelassen werden müssen. Alsdann macht derselbe übrigens nur eine Spezialität des allgemeinen Falles aus, wo die Determinante und die Grössen P_0, Q_0 komplex sind. In dieser Allgemeinheit werden wir unsere Aufgabe im zehnten Abschnitte behandeln. Vorläufig beschränken wir uns auf den angezeigten speziellen Fall, indem wir unter den Quotienten nur reelle Zahlen und zwar, wenn es sich um eine Entwickelung mit grössten Subquotienten handelt, die grössten in $\frac{\sqrt{-D}+P_n}{Q_n}$ enthaltenen reellen Ganzen, welche offenbar die in $\frac{P_n}{Q_n}$ enthaltenen Ganzen sind, aufnehmen. Im Übrigen bewirken wir die Entwickelung genau nach §. 59, setzen auch voraus, dass $Q_{-1}=\frac{-D-P_0^2}{Q_0}=-\frac{D+P_0^2}{Q_0}$ eine ganze Zahl sei.

Dies gibt z. B. für $K=\frac{\sqrt{-8}-10}{27}$, wofür

$Q_{-1}=\frac{-8-(-10)^2}{27}=-4$ ist,

$$x_0=\frac{\sqrt{-8}-10}{27}=-1+\frac{1}{x_1}$$

$$x_1=\frac{27}{\sqrt{-8}+17}=\frac{27(\sqrt{-8}-17)}{-297}=\frac{\sqrt{-8}-17}{-11}=1+\frac{1}{x_2}$$

$$x_2=\frac{-11}{\sqrt{-8}-6}=\frac{-11(\sqrt{-8}+6)}{-44}=\frac{\sqrt{-8}+6}{-4}=1+\frac{1}{x_3}$$

$$x_3=\frac{4}{\sqrt{-8}+2}=\frac{4(\sqrt{-8}-2)}{-12}=\frac{\sqrt{-8}-2}{-3}=0+\frac{1}{x_4}$$

$$x_4=\frac{-3}{\sqrt{-8}-2}=\frac{-3(\sqrt{-8}+2)}{-12}=\frac{\sqrt{-8}+2}{4}=0+\frac{1}{x_5}$$

$$x_5=\frac{4}{\sqrt{-8}+2}=\frac{4(\sqrt{-8}-2)}{-12}=\frac{\sqrt{-8}-2}{-3}=x_3$$

also $K=[-1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0\ldots]$ und

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-4		1	0
0	-10	27	-1	-1	1
1	-17	-11	1	0	1
2	6	4	1	-1	2
3	-2	-3	0	0	1
4	2	4	0	-1	2
5	-2	-3	0	0	1
6	2	4	0	-1	2

Die Entwickelung wird zuletzt periodisch, indem die folgenden Quotienten sämmtlich $=0$ werden, was zur Folge hat, dass auch die Zähler und Nenner der Näherungsbrüche Perioden bilden.

Wenn $P_0=0$ und $Q_0=1$ ist; so findet sich leicht die Entwickelung

$$K=\sqrt{-D}=\frac{\sqrt{-D}+0}{1}=[0,\ 0,\ 0,\ 0\ldots]$$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		$-D$		1	0
0	0	1	0	0	1
1	0	$-D$	0	1	0
2	0	1	0	0	1
3	0	$-D$	0	1	0

II. Es leuchtet ein, dass für die durch eine solche Entwickelung entstehenden Grössen die Formeln §. 61, Gl. (1) bis (12), §. 67, §. 68 Gl. (1) bis (6) und (11) bis (17) volle Gültigkeit behalten, dass jedoch die für reelle Wurzelgrössen gefundenen Gesetze der Periodizität eine wesentliche Änderung erleiden, auch dass sich auf die gegenwärtige Entwickelung, welche den gegebenen Ausdruck K durchaus nicht erschöpft, die Reduktionsformel des §. 58 nicht in Anwendung bringen lässt. Wegen der periodischen Wiederkehr der Näherungsbrüche selbst würde sich die Gl. (5) in §. 58 stets auf die unbestimmte Form $0.K^2-0.K+0=0$ reduziren.

§. 95. Gesetze der Periodizität der obigen Entwickelung.

I. Nach §. 61 hat man hier,

(1) $P_{n+1}=a_n\,Q_n-P_n$ (2) $Q_n\,Q_{n+1}=-(D+P_{n+1}^2)$

(3) $Q_{n+1}-Q_{n-1}=a_n\,(P_n-P_{n+1})$

und zur Bestimmung des Quotienten a_n

(4) $y_n=\frac{P_n}{Q_n}=a_n+\frac{R_n}{Q_n}$ (5) $P_n=a_n\,Q_n+R_n$

worin $\frac{R_n}{Q_n}$ positiv und <1 ist, sodass also R_n dasselbe Zeichen wie Q_n hat, sobald es sich um eine Entwickelung mit **grössten Subquotienten** handelt.

Vergleicht man die Gl. (1), wonach auch $P_n=a_n\,Q_n-P_{n+1}$ ist, mit Gl. (5); so ergibt sich sofort

(6) $P_{n+1}=-R_n$

II. Aus Gl. (2) erhellet, dass unter allen Umständen, auch wenn nicht mit grössten Subquotienten entwickelt wird, zwei benachbarte Grössen Q, also Q_n und Q_{n+1}, entgegengesetzte Zeichen haben. Entwickelt man mit grössten Subquotienten; so hat nach Gl. (6) P_{n+1} das entgegengesetzte Zeichen von R_n, also auch von Q_n. Da nun Q_{n+1} ebenfalls das entgegengesetzte Zei-

chen von Q_n hat; so haben P_{n+1} und Q_{n+1} gleiche Zeichen, und die zusammengehörigen Werthe von P und Q wechseln beide zusammen regelmässig das Zeichen, wenn der Zeiger um 1 wächst. Demnach ist, wenn nicht schon vom Zeiger 0, doch vom Zeiger 1 an, der Bruch $\frac{P_n}{Q_n}$ positiv; folglich alle Quotienten $a_1, a_2, \ldots$ positiv oder theilweise $= 0$.

III. Da nach Gl. (5), absolut genommen, $R_n \leqq P_n$ ist; so ist wegen Gl. (6), absolut genommen, $P_{n+1} \leqq P_n$. Also ist der absolute Werth jedes folgenden P entweder gleich oder kleiner, als der des vorhergehenden P.

Dies führt vermöge der Beziehung

$$(7) \qquad Q_{n+1} = -\frac{(D+P_{n+1}^2)}{Q_n} = \left(\frac{D+P_{n+1}^2}{D+P_n^2}\right) Q_{n-1}$$

zu dem Satze, dass, absolut genommen, $Q_{n+1} \leqq Q_{n-1}$ sei. Also ist der absolute Werth jedes Q gleich oder kleiner als der absolute Werth des um zwei Glieder voranstehenden Q.

IV. Da der absolute Werth keines späteren P grösser werden kann, als der eines früheren; so folgt, dass in der Entwickelung mit grössten Subquotienten eine Stelle erreicht werden muss, von wo an alle folgenden Grössen P denselben absoluten Werth haben und abwechselnd positiv und negativ sind. Angenommen, es sei

$$(8) \qquad P_n = -P_{n+1} = P_{n+2} = -P_{n+3} = \text{etc.}$$

so muss wegen Gl. (7) gleichzeitig

$$(9) \qquad Q_{n-1} = Q_{n+1} = Q_{n+3} = Q_{n+5} = \text{etc.}$$

und

$$(10) \qquad Q_n = Q_{n+2} = Q_{n+4} = Q_{n+6} = \text{etc.}$$

sein. Gleichzeitig haben die P und Q von paaren Zeigern einerlei Zeichen und die von unpaaren Zeigern das entgegengesetzte Zeichen. Das letztere Gesetz beginnt sogar schon mit dem Zeiger $n = 1$, und für die Grössen Q schon mit dem Zeiger $n = 0$, sodass die Grössen $Q_0, Q_2, Q_4 \ldots$ das Zeichen von Q_0, und die Grössen $Q_{-1}, Q_1, Q_3 \ldots$ das Zeichen von Q_{-1} haben. Auch folgt hieraus, dass die Grössen $(-1)^{-1} Q_{-1}$, $(-1)^0 Q_0$, $(-1)^1 Q_1$, $(-1)^2 Q_2 \ldots (-1)^n Q_n$ sämmtlich das Zeichen von Q_0 haben.

Ferner folgt aus Gl. (3), dass unter den obigen Umständen

$$(11) \qquad a_n = a_{n+1} = a_{n+2} = a_{n+3} = \text{etc.} = 0$$

ist, dass also alle Brüche

$$(12) \qquad \frac{P_n}{Q_n}, \frac{P_{n+1}}{Q_{n+1}}, \frac{P_{n+2}}{Q_{n+2}}, \frac{P_{n+3}}{Q_{n+3}} \text{ etc.} < 1$$

sind, oder dass der absolute Werth eines jeden Q in der Periode grösser ist, als der des P.

Die Periode der Grössen P, Q ist also zweigliederig, während die der Quotienten eingliederig ist.

V. Aus der Abnahme der absoluten Werthe der um je zwei Glieder voneinander abstehenden Grössen Q bis zur ersten Periode leuchtet ein, dass ausserhalb der Periode kein Q vorkommen kann, dessen absoluter Werth kleiner wäre, als der kleinste der beiden periodischen absoluten Werthe von Q.

VI. Die absoluten Werthe der Grössen P und Q in der Periode können gewisse Gränzen nicht übersteigen. Diese Gränzen sind folgendermaassen zu bestimmen. Wenn p der absolute Werth der periodischen Grössen P, ferner q, q' die absoluten Werthe der periodischen Grössen Q bezeichnen; so ist nach Obigem

$$q \geqq p+1 \text{ und auch } q' \geqq p+1, \text{ also}$$
$$qq' \geqq (p+1)^2 \text{ oder } \geqq p^2+2p+1$$

Nun hat man aber nach Gl. (2) $qq' = D+p^2$ folglich

$$p^2+2p+1 \leqq D+p^2, \text{ und hieraus folgt}$$

$$(13) \qquad p \leqq \frac{D-1}{2}$$

oder genauer, wenn D paar ist, $p \leqq \frac{D}{2} - 1$ und wenn D unpaar ist, $p \leqq \frac{D-1}{2}$.

Was die Gränzen von q und q' betrifft; so hat man hiernach wegen der Beziehung $qq' = D+p^2$

$$(14) \qquad qq' \leqq D + \left(\frac{D-1}{2}\right)^2 \text{ oder } \leqq \left(\frac{D+1}{2}\right)^2$$

oder genauer, nach den obigen genaueren Gränzwerthen von p, wenn D paar ist, $qq' \leqq \left(\frac{D}{2}\right)^2 + 1$ und wenn D unpaar ist, $qq' \leqq \left(\frac{D+1}{2}\right)^2$.

Ist nun q entweder $= q'$ oder gleich dem kleineren der beiden Werthe q, q'; so ist nach Gl. (14) für das Minimum der periodischen Grössen Q

$$(15) \qquad q \leqq \frac{D+1}{2}$$

oder genauer, wenn D paar ist, $q \leqq \frac{D}{2}$ und wenn D unpaar ist, $q \leqq \frac{D+1}{2}$.

§. 96. *Absolutes Minimum von Q und Periode in kleinsten Zahlen.*

I. Im vorstehenden Paragraphen haben wir gezeigt, dass das Minimum der Grössen Q in der Periode $\leqq \frac{D+1}{2}$ sein

müsse, während das zugehörige P dasselbe Zeichen wie Q hat und $\leqq \frac{D-1}{2}$ ist. Es ist damit jedoch keineswegs gesagt, dass der kleinste Werth, welchen Q überhaupt anzunehmen fähig ist, nothwendig in der nach §. 94 sich erzeugenden Periode liegen müsse. Um dieses absolute Minimum von Q, welches $= Q_n$ sei, zu bestimmen, betrachten wir die Gl. (4) des §. 68, also indem wir darin $-D$ für D setzen, die Gleichung

(1) $$(-1)^n Q_0 Q_n = (M_{n-1} Q_0 - N_{n-1} P_0)^2 + N_{n-1}^2 D$$

Die rechte Seite hierin stellt ebensowol wie die linke Seite eine positive Grösse dar, da nach §. 95 $(-1)^n Q_n$ dasselbe Zeichen hat, wie $(-1)^0 Q_0$ oder Q_0.

Soll nun Q_n ein Minimum sein; so muss es auch $Q_0 Q_n$ sein. Die Bedingung des Minimums erfordert aber nicht bloss, dass $Q_0 Q_n$ wachse, wenn M_{n-1} oder N_{n-1} oder Beide wachsen, sondern auch, dass $Q_0 Q_n$ wachse, wenn M_{n-1} oder N_{n-1} oder Beide abnehmen. Da nun, wenn N_{n-1} abnimmt, das Glied $N_{n-1}^2 D$ in Gl. (1) jedenfalls auch abnimmt; so muss, wenn gleichzeitig $Q_0 Q_n$ wachsen soll, durchaus das Glied $(M_{n-1} Q_0 - N_{n-1} P_0)^2$ oder der numerische Werth von $M_{n-1} Q_0 - N_{n-1} P_0$ wachsen, wenn M_{n-1} oder N_{n-1} oder Beide abnehmen. Diese letztere Bedingung erfordert aber nach §. 16, dass wenn P_0 und Q_0 gleiche Zeichen haben, also $\frac{P_0}{Q_0}$ positiv ist, $\frac{M_{n-1}}{N_{n-1}}$ irgend ein Näherungswerth von $\frac{P_0}{Q_0}$ sei. Hätten dagegen P_0 und Q_0 entgegengesetzte Zeichen, wäre also $\frac{P_0}{Q_0}$ negativ, mithin $-\frac{P_0}{Q_0}$ positiv; so müsste für $\frac{M_{n-1}}{N_{n-1}}$ der entgegengesetzte Werth irgend eines Näherungsbruches von $-\frac{P_0}{Q_0}$ genommen werden, sodass M_{n-1} und N_{n-1} entgegengesetzte Zeichen erhalten.

II. Hieraus ergibt sich zur Bestimmung des Minimums Q_n folgende Regel. Man entwickelt den absoluten Werth des Bruches $\frac{P_0}{Q_0}$ in einen Kettenbruch mit grössten Subquotienten $a_0, a_1, a_2 \ldots$ und nimmt diese Quotienten sämmtlich positiv, wenn $\frac{P_0}{Q_0}$ positiv ist, dagegen negativ, wenn $\frac{P_0}{Q_0}$ negativ ist. Hierauf nimmt man bei der Entwickelung von $K = \frac{\sqrt{-D}+P_0}{Q_0}$ nach §. 94 resp. die Grössen $a_0, a_1, a_2 \ldots$ oder die Grössen

$-a_0$, $-a_1$, $-a_2 \ldots$ als willkürliche Quotienten an. Der hierdurch sich ergebende numerisch kleinste Werth von Q ist das gesuchte Minimum Q_n.

Wenden wir diese Regel auf das Beispiel $K = \frac{\sqrt{-8} - 10}{27}$ des §. 94 an; so haben wir $\frac{P_0}{Q_0} = -\frac{10}{27}$ und da $\frac{10}{27} = [0, 2, 1, 2, 3]$ ist; so nehmen wir als willkürliche Quotienten $0, -2, -1, -2, -3$ an. Dies gibt

$$x_0 = \frac{\sqrt{-8} - 10}{27} = 0 + \frac{1}{x_1}$$

$$x_1 = \frac{27}{\sqrt{-8} - 10} = \frac{27(\sqrt{-8} + 10)}{-108} = \frac{\sqrt{-8} + 10}{-4} = -2 + \frac{1}{x_2}$$

$$x_2 = \frac{-4}{\sqrt{-8} + 2} = \frac{-4(\sqrt{-8} - 2)}{-12} = \frac{\sqrt{-8} - 2}{3} = -1 + \frac{1}{x_3}$$

$$x_3 = \frac{3}{\sqrt{-8} + 1} = \frac{3(\sqrt{-8} - 1)}{-9} = \frac{\sqrt{-8} - 1}{-3} = -2 + \frac{1}{x_4}$$

$$x_4 = \frac{-3}{\sqrt{-8} - 7} = \frac{-3(\sqrt{-8} + 7)}{-57} = \frac{\sqrt{-8} + 7}{19} = -3 + \frac{1}{x_5}$$

$$x_5 = \frac{19}{\sqrt{-8} + 64} = \frac{19(\sqrt{-8} - 64)}{-4104} = \frac{\sqrt{-8} - 64}{-216}$$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-4		1	0
0	-10	27	0	0	1
1	10	-4	-2	1	-2
2	-2	3	-1	-1	3
3	-1	-3	-2	3	-8
4	7	19	-3	-10	27
5	-64	-216			

Da unter dieser Reihe der Q die Grösse $Q_2 = 3$ und $Q_3 = -3$ den kleinsten numerischen Werth 3 besitzen; so bezeichnet dieses das gesuchte Minimum Q_n. Die entsprechenden Werthe von M_{n-1} und N_{n-1} sind resp. 1 und -2 oder -1 und 3.

III. Dass dieses Minimum von $Q \leqq \frac{D+1}{2}$ sein müsse, leuchtet aus §. 95 ein. Bricht man nun die vorstehende Entwickelung von K an der Stelle ab, wo man vermittelst des vorhergehenden Quotienten a_{n-1} das Minimum Q_n gefunden hatte, und setzt die fernere Rechnung nach der Vorschrift des §. 94 mit grössten Subquotienten des reellen Theiles fort, sodass also schon für a_n der grösste Subquotient von $\frac{P_n}{Q_n}$ unter gehöriger Be-

rücksichtigung der Zeichen von P_n, Q_n genommen wird; so müssen nach §. 95 die Grössen P_{n+1} und Q_{n+1} gleiche Zeichen annehmen. Ausserdem muss der absolute Werth von P_{n+1} gleich dem von R_n, also entschieden kleiner als der von Q_n, also $\leqq Q_n - 1$ d. i. $\leqq \frac{D-1}{2}$ sein. Demnach ist auch der numerische Werth des Produktes

$$Q_n\, Q_{n+1} = D + P_{n+1}^2 \leqq D + \left(\frac{D-1}{2}\right)^2, \text{ d. i. } \leqq \left(\frac{D+1}{2}\right)^2$$

und es ist, weil Q_n das Minimum der Grössen Q darstellt, numerisch genommen, $Q_{n+1} \geqq Q_n > P_{n+1}$, also $\frac{P_{n+1}}{Q_{n+1}}$ ein positiver echter Bruch.

IV. Vergleicht man diese Beziehungen mit den Resultaten des §. 95, und namentlich mit den dortigen Gleichungen (13) bis (15); so folgt, dass der eben beschriebene Übergang bei dem Quotienten a_n zu dem Entwickelungsprinzipe des §. 94 sofort vom nächsten Zeiger an die bekannte zweigliedrige Periode herstellt, wofür $a_{n+1} = a_{n+2} =$ etc. $= 0$ wird *und die* Grössen Q_{n+1}, Q_n sich abwechselnd wiederholen, während P_{n+1} konstant bleibt und nur sein Zeichen wechselt.

Man sieht leicht, dass unter Umständen zwei Entwickelungen Ein und derselben Grösse K zu verschiedenen Perioden führen können, wenn man vor Eintritt in die Periode gewisse willkürliche Quotienten einführt. So hat man z. B. für $K = \frac{\sqrt{-8} - 10}{27}$, wenn man die vorstehende Entwickelung vom Quotienten a_2 an nach §. 94 fortsetzt, was hier für den ersten Quotienten a_2 denselben Werth -1 liefert,

n	P_n	Q_n	a_n
-1		-4	
0	-10	27	0
1	10	-4	-2
2	-2	3	-1
3	-1	-3	0
4	1	3	0
5	-1	-3	0
6	1	3	0

Die Periode dieser Entwickelung ist wesentlich verschieden von der in §. 94.

V. Von allen möglichen Perioden ist nun diejenige charakteristisch, in welcher das Minimum von Q vorkommt. Diese wollen wir die Periode in kleinsten Zahlen nennen. Käme das Minimum von Q nach der obigen Ermittelung bei der Entwickelung von $\frac{P_0}{Q_0}$ in einen Kettenbruch mehrmals zum Vorschein; so wäre es denkbar, dass es mehrere Perioden mit jenem

Minimum gäbe, welche sich nach den letzteren Regeln einzeln darstellen lassen. In einem solchen Falle würden wir unter der Periode in kleinsten Zahlen diejenige verstehen, in welcher auch das zweite Q den kleinsten Werth hätte.

VI. Es leuchtet ein, dass in dem besonderen Falle $K = \frac{\sqrt{-D}}{Q_0}$, wo man $P_0 = 0$ hat, die einzig mögliche Periode in kleinsten Zahlen sich sofort durch die Entwickelung nach §. 94 ergibt, denn es ist hier $\frac{P_0}{Q_0} = \frac{0}{Q_0}$ (ein Bruch, welcher auf kleinster Bennennung $= \frac{0}{1}$ ist) als Kettenbruch $= [0]$. Die Einführung dieses einzigen Quotienten $a_0 = 0$ entspricht aber hier genau der Entwickelung nach §. 94 und stellt sofort die Periode Q_0, Q_{-1} her.

VII. Auch folgt hieraus, dass wenn man durch die Entwickelung von K nach §. 94 auf eine Periode stösst, in welcher $P_n = 0$ ist, Dies jedenfalls die einzig mögliche Periode in kleinsten Zahlen ist.

VIII. Über das Zeichen der Grössen Q haben wir noch Folgendes zu bemerken. Man hat es zwar in seiner Gewalt, nachdem unter den Grössen Q irgend ein positiver oder negativer Werth Q_n vorgekommen ist, den entgegengesetzten Werth $-Q_n$ hervorzubringen. Man braucht zu diesem Ende nur für die Quotienten a_n, a_{n+1}, a_{n+2} die Zahlen $1, -1, 1$ anzunehmen. Hierdurch wird nothwendig

$$Q_{n+3} = -Q_n \text{ also } (-1)^{n+3} Q_{n+3} = (-1)^n Q_n, \text{ ferner}$$
$$P_{n+3} = P_n$$

Dies erkennt man aus den Gleichungen (2), (1) des §. 68, wenn man beachtet, dass

$$[a_0, a_1 \ldots a_{n-2}] = \frac{M_{n-2}}{N_{n-2}}, \quad [a_0, a_1 \ldots a_{n-1}] = \frac{M_{n-1}}{N_{n-1}}$$
$$[a_0, a_1 \ldots a_{n-1}, 1, -1] = \frac{-M_{n-2}}{-N_{n-2}}, \quad [a_0, a_1 \ldots a_{n-1}, 1, -1, 1] = \frac{M_{n-1}}{N_{n-1}}$$

ist. Überhaupt wird eine Umkehrung des Zeichens von Q eine Veränderung des Zeigers um eine unpaare Zahl zur Folge haben, indem das zugehörige P, wenn dasselbe numerisch seinen Betrag nicht ändert, auch das frühere Zeichen behält.

Lag nun das frühere P und Q in der Periode; so kann das spätere P und Q nicht in einer Periode liegen, weil nun $\frac{P}{Q}$ negativ sein würde. Nur wenn $P = 0$ ist, wäre Dies möglich.

Man kann also eine Periode, worin P und Q das Entgegengesetzte von zwei in einer anderen Periode liegenden Grössen

dieser Art sein sollen, nur dann erzeugen, wenn $P = 0$ ist, oder zuweilen auch dann, wenn es mehrere Perioden in kleinsten Zahlen gibt, von denen irgend zwei in der gewünschten Beziehung zu einander stehen.

IX. Durch die Bestimmung der Perioden in kleinsten Zahlen ist man in den Stand gesetzt, zu untersuchen, ob sich zwei Grössen K und K' mit derselben Determinante $-D$ zu Ein und derselben Periode führen lassen oder nicht, also auch, ob dieselben nach §. 73 kombinirt werden können. Die Thunlichkeit einer solchen Kombination setzt hier wie dort nur die Übereinstimmung zweier zusammengehöriger Werthe wie P_n, Q_n mit P'_n, Q'_n voraus, indem alsdann nothwendig auch Q_{n-1} mit Q'_{n-1} übereinstimmen muss.

Bei Übereinstimmung der Perioden kann man bei jedem Periodengliede die Kombination ausführen. Da jedoch hier alle Quotienten der Periode $=0$ sind; so leuchtet ein, dass es hinsichtlich der hierbei entstehenden Grössen M, N, welche die Endwerthe einer jeden Kombination bilden, ganz gleichgültig ist, bei welchen Zeigern in der Periode man kombinirt; es besteht hier die in §. 83 betrachtete unendliche Reihe der Werthe für M, N aus lauter gleichen Grössen.

§. 97. *Entwickelung der Grösse K mit Quotienten, welche den reellen Theil der Grössen x_0, x_1, x_2... am vollständigsten erschöpfen.*

Auch im gegenwärtigen Falle, wo die Determinante $-D$ negativ ist, ist es von Interesse, die in §. 69 für eine positive Determinante angestellte Entwickelung zu betrachten, wonach man in der Formel

$$x_n = \frac{\sqrt{-D} + P_n}{Q_n} = a_n + \frac{1}{x_{n+1}}$$

für den Quotienten a_n stets die dem Bruche $\frac{P_n}{Q_n}$ am nächsten kommende ganze Zahl nimmt.

Die Resultate sind den in §. 69, I. bis V. gefundenen ganz gleich. Es erzeugt sich auch hier eine zweigliederige Periode, in welcher man numerisch

$$(1) \qquad P_{n+1} \leqq \tfrac{1}{2} Q_n \text{ und auch } \leqq \tfrac{1}{2} Q_{n+1}$$

$$\text{und } a_{n+1} = a_{n+2} = a_{n+3} = \ldots = 0 \text{ hat.}$$

Was jedoch die Gränzwerthe der periodischen Grössen P und Q betrifft; so folgt aus der allgemeinen Beziehung $Q_n Q_{n+1} = -(D + P_{n+1}^2)$, dass die Summe

$$D + P_{n+1}^2 \geqq 4 P_{n+1}^2$$

dass also

(2) $$D \geqq 3 P_{n+1}^2 \text{ oder } P_{n+1} \leqq \sqrt{\frac{D}{3}}$$

sei.

Ferner folgt aus jener allgemeinen und aus der letzteren Beziehung, dass die beiden periodischen Grössen Q_n und Q_{n+1} entgegengesetzte Zeichen haben, dass aber numerisch $Q_n Q_{n+1} \leqq D + \frac{D}{3}$ d. i. $\leqq \frac{4D}{3}$, dass mithin der numerische Werth der Einen von beiden $\leqq \sqrt{\frac{4D}{3}}$ ist.

§. 98. ***Zahlenreihe, welche im Stande ist, die bei der Entwickelung der Grösse K mit negativer Determinante vorkommenden Operationen zu ersetzen.***

I. Die allgemeinen Resultate der §§. 75 bis 81 finden auch hier ihre Anwendung. Die Zahlen $J_p = -J - p^2 = -(J + p^2)$ sind hier sämmtlich negativ, ohne dass Eine $= 0$ wäre. Die dortige Gränzlinie $\alpha\alpha$ zwischen den positiven und negativen Zahlen ist hier, als über dem höchsten Gliede J_0 liegend, zu denken. Bei einer Entwickelung mit grössten Subquotienten oszillirt die Bewegung jedenfalls schon vom Zeiger 1 an fortwährend um das Glied J_0, und in der Periode kann das Glied mit dem Zeiger $p = \frac{D-1}{2}$ nicht überschritten werden.

Alles Dieses kann man an dem in §. 94 bis 96 erörterten Beispiele mit der Determinante -8 und der Zahlenreihe

α——————————————————————α

	J_0	$-8-0^2$	-8	$-1.2.2.2$
J_{-1}	J_1	$-8-1^2$	-9	$-1.3.3$
J_{-2}	J_2	$-8-2^2$	-12	$-1.2.2.3$
J_{-3}	J_3	$-8-3^2$	-17	-1.17
J_{-4}	J_4	$-8-4^2$	-24	$-1.2.2.2.3$
J_{-5}	J_5	$-8-5^2$	-33	$-1.3.11$

u. s. w.

spezieller prüfen.

II. Die Methoden der §§. 76, 77 ff. sind auch hier anwendbar, um die Reihen der durch eine gegebene Zahl q theilbaren Zahlen J aufzufinden. Es muss auch hier für Ein Glied jeder Reihe, wenn q paar ist, $p \leqq \frac{q}{2}$ und wenn q unpaar ist, $p \leqq \frac{q-1}{2}$ sein.

Setzen wir hier überall $-D$, wo in den dortigen Paragraphen D steht; so muss man nach der Methode des §. 77 auch hier

$$-D - rq = p^2$$

haben, woraus folgt, dass r und q jedenfalls entgegengesetzte Zeichen besitzen müssen. Setzt man also, was immer geschehen kann, q als positiv voraus; so muss r negativ sein. Man kann nun buchstäblich nach der Vorschrift des §. 77 verfahren, indem man auch hier für

r_0 den grössten Subquotienten von $-\frac{D}{q}$ und für

r_1 den kleinsten Superquotienten von $-\frac{D+\left(\frac{q}{2}\right)^2}{q}$ oder

$-\frac{D+\left(\frac{q-1}{2}\right)^2}{q}$, jenachdem q paar oder unpaar ist, annimmt.

III. Beispiel. Es sei $-D=-8$, $q=24$, also q paar und $\frac{q}{2}=12$. Hier ist $-\frac{D}{q}=-\frac{8}{24}$, $-\frac{D+\left(\frac{q}{2}\right)^2}{q}=-\frac{8+12^2}{24}=-6\frac{8}{24}$, also $r_0=-1$, $r_1=-6$, $r_0-r_1=5$ und zuvörderst $-D-r_0q=16$.

Dies gibt folgende Rechnung

r	$-D-rq$
	$24=q$
$r_0=-1$	$16=4^2$
-2	40
-3	$64=8^2$
-4	88
-5	112
$r_1=-6$	136

Es gibt also die beiden Reihen resp. für $p=4$ und $p=8$

$\ldots J_{-20}\ J_4\ J_{28}\ldots=\ldots-408\ -24\ -792\ldots$
$\ldots J_{-16}\ J_8\ J_{32}\ldots=\ldots-264\ -72\ -1032\ldots$

und die konjugirten davon.

Man konnte übrigens in diesem Falle auch berücksichtigen, dass 24 die beiden relativ primen Faktoren $q', q''=3, 8$ besitzt, und nach §. 79 verfahren.

Entwickelung der Wurzel einer quadratischen Gleichung in einen Kettenbruch nach dem Subtraktionsprinzipe.

§. 99. ***Die wichtigsten Formeln für diese Entwickelung.***

Ebenso wie eine rationale Grösse, lässt sich auch der Ausdruck $K=\frac{\sqrt{D}+P_0}{Q_0}$, gleichviel ob derselbe rational oder irrational, reell oder imaginär ist, in einen Kettenbruch nach dem

Subtraktionsprinzipe entwickeln (§. 23). Man kann bei diesem Prinzipe ebenfalls grösste Subquotienten, kleinste Superquotienten, numerisch grösste Subquotienten und willkürliche Quotienten zulassen. Will man mit Ausnahme des ersten Quotienten a_0, welcher positiv, negativ oder null werden kann, lauter positive Quotienten erhalten; so muss man überall die kleinsten Superquotienten nehmen.

Wir setzen auch hier voraus, dass $\frac{D-P_0^2}{Q_0}$ eine ganze Zahl sei, und schreiben

(1) $$Q_{-1} = -\frac{D-P_0^2}{Q_0} = \frac{P_0^2-D}{Q_0}$$

Allgemein hat man nun nach dem Prinzipe des Kettenbruchs $a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \text{etc.}}} = [a_0,\ a_1,\ a_2, \ldots]\ (-)$

$$x_n = \frac{\sqrt{D}+P_n}{Q_n} = a_n - \frac{1}{x_{n+1}} \text{ also}$$

$$x_{n+1} = \frac{\sqrt{D}+a_n Q_n - P_n}{\frac{D-(a_n Q_n - P_n)^2}{-Q_n}} = \frac{\sqrt{D}+a_n Q_n - P_n}{\frac{D-P_n^2}{-Q_n} - 2a_n P_n + a_n^2 Q_n}$$

$$= \frac{\sqrt{D}+a_n Q_n - P_n}{Q_{n-1} - 2a_n P_n + a_n^2 Q_n} = \frac{\sqrt{D}+P_{n+1}}{Q_{n+1}} = a_{n+1} - \frac{1}{x_{n+2}}$$

Dies ergibt statt der Gl. (2), (4), (6) in §. 61 die Grundformeln

(2) $$P_{n+1} = a_n Q_n - P_n$$

(3) $$Q_{n+1} = -\frac{D-P_{n+1}^2}{Q_n} = \frac{P_{n+1}^2 - D}{Q_n}$$

(4) $$Q_{n+1} = Q_{n-1} - 2a_n P_n + a_n^2 Q_n$$

und statt der Gl. (1), (2), (3), (4), (5) in §. 68

(5) $$P_n = M_{n-1} M_{n-2} Q_0 - (M_{n-1} N_{n-2} + M_{n-2} N_{n-1}) P_0 + N_{n-1} N_{n-2} Q_{-1}$$

(6) $$Q_n = M_{n-1}^2 Q_0 - 2M_{n-1} N_{n-1} P_0 + N_{n-1}^2 Q_{-1}$$

(7) $$Q_0 P_n = (M_{n-1} Q_0 - N_{n-1} P_0)(M_{n-2} Q_0 - N_{n-2} P_0) - N_{n-1} N_{n-2} D$$

(8) $$Q_0 Q_n = (M_{n-1} Q_0 - N_{n-1} P_0)^2 - N_{n-1}^2 D$$

(9) $$N_{n-2} Q_n - N_{n-1} P_n = N_{n-1} P_0 - M_{n-1} Q_0$$

Es ist beachtenswerth, dass hier die rechten Seiten der Gl. (5) und (6) resp. die Grössen P_n und Q_n nach ihrem numerischen Werthe und nach ihrem Zeichen darstellen, was bei deren Verwendung zur Auflösung der unbestimmten Gleichungen vom zweiten Grade gewisse Vortheile hat.

Als Beispiel der Entwickelung nach dem Subtraktionsprinzipe diene der Ausdruck $K = \frac{\sqrt{11}+9}{7}$, welcher in §. 60 auch

nach dem Additionsprinzipe entwickelt ist. Hier hat man $D=11=3^2+2,\ a=3,\ Q_{-1}=-\frac{11-9^2}{7}=10$ und ferner

$$x_0=\frac{\sqrt{11}+9}{7}=2-\frac{1}{x_1}$$

$$x_1=\frac{-7}{\sqrt{11}-5}=\frac{-7(\sqrt{11}+5)}{-14}=\frac{\sqrt{11}+5}{2}=5-\frac{1}{x_2}$$

$$x_2=\frac{-2}{\sqrt{11}-5}=\frac{-2(\sqrt{11}+5)}{-14}=\frac{\sqrt{11}+5}{7}=2-\frac{1}{x_3}$$

$$x_3=\frac{-7}{\sqrt{11}-9}=\frac{-7(\sqrt{11}+9)}{-70}=\frac{\sqrt{11}+9}{10}=2-\frac{1}{x_4}$$

$$x_4=\frac{-10}{\sqrt{11}-11}=\frac{-10(\sqrt{11}+11)}{-110}=\frac{\sqrt{11}+11}{11}=2-\frac{1}{x_5}$$

$$x_5=\frac{-11}{\sqrt{11}-11}=\frac{-11(\sqrt{11}+11)}{-110}=\frac{\sqrt{11}+11}{10}=2-\frac{1}{x_6}$$

$$x_6=\frac{-10}{\sqrt{11}-9}=\frac{-10(\sqrt{11}+9)}{-70}=\frac{\sqrt{11}+9}{7}=x_0$$

$$K=\frac{\sqrt{11}+9}{7}=[\underbrace{2,\ 5,\ 2,\ 2,\ 2,\ 2},\ 2,\ 5,\ 2,\ldots]\ (-)$$

n	P_n	Q_n	a_n	M_n	N_n
-2				0	-1
-1		10		1	0
0	9	7	2	2	1
1	5	2	5	9	5
2	5	7	2	16	9
3	9	10	2	23	13
4	11	11	2	30	17
5	11	10	2	37	21
6	9	7	2	44	25
7	5	2	5	183	104

Es gibt hier für die Periodizität, wenn K reell oder imaginär, aber irrational ist, sowie für den Schluss der Entwickelung, wenn die Determinante D ein vollkommenes Quadrat, also K rational ist, ähnliche Gesetze, wie bei den Entwickelungen nach dem Additionsprinzipe. Wir müssen jedoch die speziellere Erforschung derselben dem Leser überlassen.

Nachtrag zu §. 72.

Den Gesetzen des §. 72 ist noch folgende Beziehung hinzuzufügen.

Die Periode der Grösse $K'=\frac{\sqrt{D}-P_0}{Q_0}$ ist von der der

Grösse $K = \frac{\sqrt{D}+P_0}{Q_0}$ dergestalt das Umgekehrte, dass man hat:

Periode von K				Periode von K'			
a_m	$a_{m+1} \ldots$	a_{n-1}	a_n	a_n	$a_{n-1} \ldots$	a_{m+1}	a_m
P_m	$P_{m+1} \ldots$	P_{n-1}	P_n	P_{n+1}	$P_n \ldots$	P_{m+2}	P_{m+1}
Q_m	$Q_{m+1} \ldots$	Q_{n-1}	Q_n	Q_n	$Q_{n-1} \ldots$	Q_{m+1}	Q_m

Um Dies zu beweisen, betrachten wir die Entwickelung von K bei einem in irgend einer späteren Periode liegenden Zeiger n. An dieser Stelle hat man $x_n = \frac{\sqrt{D}+P_n}{Q_n}$.

In §. 72, II ist gezeigt, dass man in der Entwickelung von K' stets das Glied $\frac{\sqrt{D}-P_{n+1}}{Q_{n+1}}$ und wenn man dann den Quotienten 0 folgen lässt, das Glied $\frac{\sqrt{D}+P_{n+1}}{Q_n}$ erzeugen kann. Setzt man jetzt die Entwickelung von K' in der Weise fort, dass man für die Quotienten sukzessive die periodischen Quotienten von K in umgekehrter Reihenfolge a_n, $a_{n-1} \ldots$ einführt; so lassen die Formeln (1) bis (4) des §. 61 und die daraus sich ergebenden allgemeinen Beziehungen

$$P_n = a_n Q_n - P_{n+1}, \qquad Q_n = \frac{D - P_{n+1}^2}{Q_{n+1}}$$

sofort erkennen, dass in der Reihe der Grössen P, Q die schon vorhin bezeichneten Werthe auftreten werden. Die eingeführten Quotienten sind aber in der That die grössten Subquotienten: denn da allgemein $\frac{\sqrt{D}+P_{n+1}}{Q_n} = a_n + \frac{\sqrt{D}-P_n}{Q_n}$, und in der Periode nach §. 61 Formel (3) $\frac{\sqrt{D}-P_n}{Q_n}$ positiv und < 1 ist; so besitzen in der Periode die beiden Grössen $\frac{\sqrt{D}+P_n}{Q_n}$ und $\frac{\sqrt{D}+P_{n+1}}{Q_n}$ stets denselben grössten Subquotienten a_n. Nach §. 70 ist also die so erzeugte Periode die der Grösse K' wirklich zukommende, und dieselbe ist nur dann gleich der von K, wenn diese symmetrisch ist.

Ferner folgt daraus und aus §. 72, IV, dass die beiden Ausdrücke $\frac{\sqrt{D}+P_0}{Q_0}$ und $\frac{\sqrt{D}+P_0}{Q_{-1}}$ umgekehrte Perioden besitzen.

Endlich ist mit Rücksicht auf §. 71 klar, dass die beiden Wurzeln $\frac{\pm\sqrt{D}+P_0}{Q_0}$ der quadratischen Gleichung

$$Q_0 x^2 - 2P_0 x - Q_{-1} = 0$$

von welchen man die zweite Wurzel $\frac{-\sqrt{D}+P_0}{Q_0} = \frac{\sqrt{D}-P_0}{-Q_0}$ setzen kann, umgekehrte Perioden haben.

Fünfter Abschnitt.

Auflösung der unbestimmten Gleichungen vom zweiten Grade mit zwei Unbekannten in ganzen Zahlen.

Gleichungen, welche ausser dem bekannten Gliede nur Glieder von zwei Dimensionen enthalten.

§. 100. *Allgemeine Auflösung dieser Gleichungen in ganzen Zahlen.*

I. Die aufzulösende Gleichung sei in die Form

(1) $$ax^2 - 2bxy - cy^2 = k$$

gebracht, worin sämmtliche Koeffizienten a, $2b$, c, k ganze Zahlen sind und der Koeffizient $2b$ von xy eine paare Zahl ist; im Übrigen können diese Grössen sowol positiv wie negativ, auch null sein. Wenn der Koeffizient xy nicht schon von vorn herein eine paare Zahl wäre, würde man die ganze Gleichung mit 2 zu multipliziren haben, um jene Bedingung zu erfüllen.

Besässen die drei Koeffizienten a, $2b$, c in den unbekannten Gliedern einen gemeinschaftlichen Faktor (mit Ausschluss von ± 1, welcher nicht auch in dem bekannten Gliede k enthalten wäre; so würde offenbar die ganze Aufgabe unmöglich sein. Befreiet man demnach die vier Zahlen a, $2b$, c, k von ihrem etwaigen gemeinschaftlichen Maasse; so müssen die ersten drei a, $2b$, c unter sich prim werden. Ist Dies der Fall; so kann man die Auflösungen, wenn es deren gibt, in folgender Weise finden.

Man muss hierbei diejenigen Auflösungen x, y, welche relativ prim sind, von denjenigen unterscheiden, welche ein gemeinschaftliches Maass haben. Wir suchen zuvörderst die ersteren auf.

II. Die Grundzüge des einzuschlagenden Verfahrens sind schon in §. 74 angegeben. Man identifizirt die gegebene Gl. (1) mit der Gl. (2) aus §. 68, nämlich mit

(2) $$Q_0 M_{n-1}^2 - 2 P_0 M_{n-1} N_{n-1} - Q_{-1} N_{n-1}^2 = (-1^n) Q_n$$

indem man setzt

(3) $$Q_0 = a, \qquad P_0 = b, \qquad Q_{-1} = \frac{D - P_0^2}{Q_0} = c$$

Wegen der Beziehung (3) besitzt die Determinante D den Werth

(4) $$D = P_0^2 + Q_0 Q_{-1} = b^2 + ac$$

und man hat

(5) $$K = \frac{\sqrt{D} + P_0}{Q_0} = \frac{\sqrt{b^2 + ac} + b}{a}$$

Wir machen noch darauf aufmerksam, dass dieser Werth von K die Wurzel x der Gleichung

(6) $$ax^2 - 2bx - c = 0$$

darstellt.

Jetzt entwickelt man K nach einem bestimmten Prinzipe, z. B. nach dem Additionsprinzipe in einen Kettenbruch. Wenn die Determinante D positiv und kein vollkommenes Quadrat ist, wird der Kettenbruch unendlich und periodisch werden. Wenn dagegen D positiv und ein vollkommenes Quadrat ist, wird der Kettenbruch schliessen; man führt ihn dann nach §. 90 oder wenn D gleich null ist, nach §. 93 zu dem Schlusse in kleinsten positiven Zahlen. Wenn endlich D negativ ist, wird der Kettenbruch unendlich werden und die bekannte zweigliederige Periode mit annullirten Quotienten annehmen; man stellt alsdann nach §. 96 die Periode in kleinsten Zahlen her.

III. Jetzt nimmt man

(7) $$q = k$$

und sucht nach §. 76 oder 77 ff. die verschiedenen Reihen der durch k theilbaren Zahlen J von der Form

(8) $$D - p^2 = kr$$

auf. Gibt es eine solche Zahl nicht; so ist die Aufgabe unmöglich. Im entgegengesetzten Falle dagegen gibt es für p eine bestimmte Anzahl positiver Werthe, welche $\leqq \frac{k}{2}$ sind. Ein jeder dieser Werthe von p ist dann noch (für die konjugirte Reihe) mit entgegengesetztem Zeichen zu nehmen. Aus jedem

dieser Werthe von p, von denen immer zwei in der Form $\pm p$ zusammengefasst werden können, bildet man die Grösse

(9) $$K' = \frac{\sqrt{D} \pm p}{k}$$

und entwickelt dieselbe ebenso wie die Grösse K in einen Kettenbruch.

IV. Stimmt von keinem dieser Werthe von K' die Periode, oder der Schluss (insofern die Determinante ein Quadrat ist) mit der Periode, resp. dem Schlusse von K überein; so ist die Aufgabe unmöglich.

Jeder Werth von K' dagegen, für welchen diese Übereinstimmung stattfindet, kann nach §. 73, 74 mit K kombinirt werden. Hierdurch findet man, wenn $K(m)$ und $K'(m')$ zwei identische Glieder von K und K' bezeichnen, indem man die Kombination $K(m)$ *komb.* $K'(m')$ bildet, dass die Grösse k unter der Reihe der Grössen Q einer Entwickelung von K erscheint. Dieselbe hat den Zeiger $m+m'$, sodass $Q_{m+m'}=k$ und $(-1)^{m+m'}Q_{m+m'}=(-1)^{m+m'}k$ ist. Die Zähler und Nenner des Näherungsbruches vom nächstvorhergehenden Zeiger $m+m'-1$, also die Zahlen $M_{m+m'-1}$, $N_{m+m'-1}$, sind alsdann von der Beschaffenheit, dass sie die Gleichung

$$Q_0 M_{m+m'-1}^2 - 2P_0 M_{m+m'-1} N_{m+m'-1} - Q_{-1} N_{m+m'-1}^2 = (-1)^{m+m'} Q_{m+m'}$$

d. i.

(10) $$a M_{m+m'-1}^2 - 2b M_{m+m'-1} N_{m+m'-1} - c N_{m+m'-1}^2 = (-1)^{m+m'} k$$

erfüllen. Diese Gleichung stimmt dann mit der gegebenen Gl. (1) überein, wenn $(-1)^{m+m'}=+1$, also wenn $m+m'$ eine paare Zahl ist, und Dies setzt voraus, dass die Zeiger m und m', bei welchen die Entwickelungen von K und K' übereinstimmen, entweder beide paar oder beide unpaar sind.

Wäre in allen Entwickelungen von jeden zwei Zeigern m und m', bei welchen Übereinstimmung stattfindet, der Eine paar und der andere unpaar; so würde trotz jener Übereinstimmung die Aufgabe unmöglich sein. Dieser Fall der Unmöglichkeit kann offenbar in solchen Fällen niemals eintreten, wo die mit K' übereinstimmende Periode von K eine unpaare Gliederzahl besitzt, weil alsdann, jenachdem man in der Kombination $K(m)$ *komb.* $K'(m')$ den Zeiger m oder m' um Eine Periodenlänge wachsen lässt, die Grösse $(-1)^{m+m'}$ auf der rechten Seite von Gl. (10) regelmässig das Zeichen wechselt, also bald positiv, bald negativ ist.

Ausser den im Vorstehenden angezeigten Umständen kann es keine geben, unter welchen die Aufgabe unmöglich würde.

Hat man es nun mit einer möglichen Aufgabe zu thun; so kommt es noch auf ein Verfahren an, mittelst dessen man durch die einfachste Rechnung alle Auflösungen in der Reihenfolge vom Kleineren zum Grösseren fin-

den kann. Dieses Verfahren muss zugleich die Überzeugung verschaffen, dass keine zwischen den gesteckten Gränzen liegende Auflösung sich der Darstellung entziehe, auch dass nicht Ein und dieselbe Auflösung unbestimmt viele Mal sich reproduziren werde. Ein solches Verfahren wollen wir sofort beschreiben.

V. Zuvörderst sei die Determinante D positiv und kein Quadrat. Wenn die Periode von K nicht symmetrisch ist, wird von je zwei durch die Formel (9) dargestellten Werthen von K', welche bekanntlich umgekehrte Perioden besitzen, höchstens ein einziger eine mit K kombinirbare Entwickelung liefern. Für irgend einen brauchbaren Werth von K' besitze die übereinstimmende Periode von K und K' r Glieder und m, m' seien die höchsten Zeiger in der ersten Periode resp. von K und K'. Ist r paar; so kann die Kombination von K und K' nur dann Auflösungen liefern, wenn m und m' entweder beide paar oder beide unpaar sind. Ist r unpaar; so werden sich zwar immer Auflösungen aus jener Kombination ergeben: es ist jedoch darauf zu achten, dass bei jeder Kombination m und m' entweder beide paar oder beide unpaar sein müssen. Fände Dies nicht schon bei den höchsten Zeigern der ersten Periode von K und K' statt; so sei m der höchste Zeiger der ersten Periode von K und m' der höchste Zeiger der zweiten Periode von K', oder umgekehrt. Man hat aber in allen Fällen, wo die Gliederzahl der Periode unpaar ist, damit $m+m'$ eine paare Zahl sein könne, nothwendig je zwei Perioden zu einer einzigen zusammenzufassen, sodass nunmehr r die doppelte Gliederzahl als vorhin bezeichnet.

Aus Vorstehendem leuchtet ein, dass man immer, gleichviel, ob die Gliederzahl der Periode der Grössen P_n, Q_n, a_n paar oder unpaar sei, unter r die Gliederzahl der Periode der Grössen $(-1)^n Q_n$ verstehen könne, welche stets paar sein wird. m und m' sind immer die höchstmöglichen Zeiger innerhalb dieser Periode, für welche die Übereinstimmung zwischen K und K' stattfindet, und für welche die Summe $m+m'$ paar ist.

Nun bildet man nach §. 73 und 84 die Kombinationen

(11) $K(m)$, $(m+r)$, $(m+2r)$, $(m+3r)\ldots$ *komb.* $K'(m')$

(12) $K(m)$ *komb.* $K'(m')$, $(m'+r)$, $(m'+2r)$, $(m'+3r\ldots$

welche nach §. 84 eine einzige zusammenhängende Reihe von Auflösungen ergeben, deren numerische Beträge von der Mitte nach beiden Seiten hin eine steigende Progression bilden. Da hierin r stets eine paare Zahl, also $(-1)^{r-1}=-1$ ist; so werden die Rekursionsformeln (19) und (20) in §. 84 stets nach dem Subtraktionsprinzipe gebildet sein. Auch wird die bloss von der Periode von K abhängige Grösse h für alle Kombinationsreihen Ein und denselben Werth behalten.

Obgleich hiernach die Werthe von x und y ins Unendliche wachsen; so nähert sich doch offenbar das Verhältniss $\frac{x}{y} = \frac{M}{N}$ einer bestimmten Gränze. Dies lehrt auch die Gl. (1), wenn man dieselbe durch y^2 dividirt, wodurch sich

(13) $$a\left(\frac{x}{y}\right)^2 - 2b\left(\frac{x}{y}\right) - c = \frac{k}{y^2}$$

ergibt. Hieraus ersieht man, dass für ein unendlich grosses y die Grösse $\frac{k}{y^2} = 0$, also das Verhältniss $\frac{x}{y}$ gleich der Wurzel der Gl. (6) wird. Nun ist leicht zu zeigen, dass sich das Verhältniss $\frac{x}{y}$ aus der Reihe der Kombinationen (11) dem Werthe

(14) $$\frac{x}{y} = \frac{+\sqrt{D} + P_0}{Q_0} = \frac{+\sqrt{b^2 + ac} + b}{a}$$

dass sich dagegen dieses Verhältniss aus der Reihe der Kombinationen (12) dem Werthe

(15) $$\frac{x}{y} = \frac{-\sqrt{D} + P_0}{Q_0} = \frac{-\sqrt{b^2 + ac} + b}{a}$$

fortwährend nähert.

VI. Es ist nun wichtig, dass keine denkbare Kombination zwischen K und K' eine andere Auflösung erzeugen kann, welche nicht schon in der Reihe (11), (12) vorkäme. Der Beweis dieses Satzes ist aus §. 73 zu abstrahiren, und wir heben dabei hervor, dass es ganz gleichgültig ist, ob in K und K' vor den Perioden übereinstimmende Glieder liegen oder nicht. Der Umstand, dass man in manchen Fällen die erste Periode ebenso gut bei einem früheren, wie bei einem späteren Gliede beginnen kann, hat ebenfalls keinen Einfluss auf den vorstehenden Satz.

VII. Es kann sich ereignen, dass unter den Grössen $(-1)^n Q_n$ der Entwickelung von K selbst schon der Werth k vorkommt. Alsdann liefert also diese Entwickelung ohne alle weitere Kombination mit K' für sich allein schon Auflösungen der Gl. (1), und zwar eine endliche Menge, wenn k vor der Periode der Grössen $(-1)^n Q_n$ vorkommt, und eine unendliche Menge, wenn k in der Periode dieser Grössen vorkommt.

Es ist nun ferner wichtig, dass man die zuletzt erwähnten Auflösungen, welche nicht als ein Resultat der Kombinationen (11), (12) zwischen K und K' erscheinen, sämmtlich ausser Acht lassen kann, indem sich dieselben nothwendig irgendwo unter den Kombinationen von K mit den verschiedenen möglichen Werthen von K' einstellen werden.

Um diesen Satz zu erläutern, machen wir zunächst auf folgende ebenfalls sehr wichtige Thatsache aufmerksam. Wenn p Eine von den Zahlen ist, für welche $D-p^2=kr$ durch k theilbar wird; so brauchen einzig und allein diejenigen positiven und negativen Werthe von p in den Ausdruck

$$K'=\frac{\sqrt{D}+p}{k}$$

gesetzt zu werden, deren numerische Beträge $\leqq\frac{k}{2}$ sind. Denn jeder Werth von p, für welchen dieser Betrag $>\frac{k}{2}$ ist, kann in die Form $p+wk$ gebracht werden, worin $p\leqq\frac{k}{2}$ ist. Die Kettenbruchsentwickelung von $\frac{\sqrt{D}+p+wk}{k}$ $=w+\frac{\sqrt{D}+p}{k}$ unterscheidet sich aber nur durch den Werth des ersten Quotienten a'_0 von der Entwickelung der Grösse $K'=\frac{\sqrt{D}+p}{k}$. Dieser erste Quotient a'_0 tritt aber niemals mit in die Kombination $K(m)$ *komb.* $K'(m')$ ein, indem an die Quotienten $a_0, a_1 \ldots a_{m-1}$ der Grösse K die Quotienten $0, -a'_{m'-1}, -a'_{m'-2} \ldots -a'_1$ gehängt werden; und für den speziellen Fall, wo $m'=0$ wäre, $K(m)$ *komb.* $K'(0)=K(m)$ ist.

Gibt es nun unter den Grössen $(-1)^n Q_n$ der Entwickelung von K irgendwo einen Werth $=k$, welcher der Stelle

$$x_n=\frac{\sqrt{D}+P_n}{Q_n}=a_n+\frac{1}{x_{n+1}}$$

entsprechen möge; so ist M_{n-1}, N_{n-1} eine Auflösung der gegebenen Gl. (1). Allein diese Auflösung muss nothwendig in einer Kombination von K mit irgend Einem der Werthe von K' vorkommen. Denn es ist klar, dass wegen der vorstehenden Beziehung entweder $P_n=p$ oder $P_n=p+wk$ sein muss, worin $p\leqq\frac{k}{2}$ ist. Wäre $P_n=p$; so käme P_n unter den Grössen p vor, welche die Ausdrücke K' bilden, und für diesen Ausdruck von K', welcher jedenfalls schon vom Zeiger 0 an mit K übereinstimmen müsste, würde die Kombination

$$K(n) \text{ komb. } K'(0)=K(n)$$

sofort zu derselben Auflösung M_{n-1}, N_{n-1} führen. Wäre aber $P_n=p+wk$; so würde es unter den Grössen p, welche die Ausdrücke K' bilden, Eine geben, für welche die Entwickelung von K' vom Zeiger 1 an, genau mit der von K übereinstimmte. In diesem Falle würde die Kombination

$$K(n+1) \; komb. \; K'(1)$$

sofort die in Rede stehende Auflösung M_{n-1}, N_{n-1} liefern.

Demnach erhält man alle Auflösungen der Gl. (1), indem man zwischen K und jedem zulässigen Werthe von K' die nach beiden Seiten ins Unendliche sich fortsetzende Reihe der Kombinationen (11), (12) bildet, was nach §. 84 mit dem geringst möglichen Rechenaufwande geschehen kann.

In dem eben betrachteten Falle, wo die Determinante $D = b^2 + ac$ positiv und kein vollkommenes Quadrat, also K reell und irrational ist, gibt es also entweder keine oder unendlich viele Auflösungen.

VIII. Ist die Determinante D ein positives Quadrat d^2 verschieden von null; so hat man in der Kombination $K(m)$ *komb.* $K'(m')$ unter m und m' die Zeiger der höchsten übereinstimmenden Glieder von K und K' zu verstehen. Es müssen auch hier m und m' entweder beide paar oder beide unpaar sein. In diesem Falle liefert die Kombination zwischen K und K' immer nur eine einzige Auflösung (§. 73). Alle gelegentlichen Auflösungen, welche sich etwa schon in der Entwickelung von K herausstellen, kann man auch hier ausser Acht lassen, wenn man nach und nach die verschiedenen zulässigen Werthe von K' berücksichtigt. Wenn in diesem Falle $k = 0$ ist; so stösst man für $p = \pm d$ auf die Form $K' = \frac{\sqrt{d^2} \pm d}{0}$, welcher nach §. 91 $d+1$ verschiedene Werthe beizulegen sind. Die Anzahl der Auflösungen ist in vorstehendem Falle immer endlich. Man darf übrigens nicht übersehen, dass sich nach §. 90, III der Schluss in kleinsten positiven Zahlen von K oder K' zuweilen nach einer unpaaren Gliederzahl nochmals reproduziren lässt.

IX. Ist ferner die Determinante D gleich null; so hat man das im vorhergehenden Falle für $D = d^2$ beschriebene Verfahren zu beobachten. Es ist aber wichtig, dass man nach §. 93 den bereits erreichten Schluss in kleinsten positiven Zahlen bei einem um 2 Einheiten grösseren Zeiger noch einmal reproduziren kann, indem man auf den letzten Quotienten die beiden Quotienten w und 0 folgen lässt, wovon w ganz willkürlich ist. Hierdurch tritt in den Werth von $M = x$ und $N = y$ eine willkürliche Grösse w auf erster Potenz ein, und die aus der Kombination von K und K' gefundene Auflösung repräsentirt demzufolge eine unendliche Menge von Auflösungen, welche man sämmtlich erhält, wenn man w in der Reihe der ganzen Zahlen ... $-2, -1, 0, 1, 2$ ... variiren lässt. Im Übrigen sind keine neuen Auflösungen daraus zu erwarten, dass man auch den Schluss von K' in jener Weise durch eine willkürliche Zahl w' oder die Schlüsse von

K und K' nach dem Prinzipe des §. 93 durch mehr als Eine solche willkürliche Zahl zu wiederholten Malen reproduzirt, ehe man die Kombination von K und K' eintreten lässt, indem die hieraus entstehenden Auflösungen ebenso zusammengesetzt sind, wie die zuerst bezeichnete, mit dem unwesentlichen Unterschiede, dass an der Stelle der Einen Willkürlichen w die Summe mehrerer anderen Willkürlichen $w+w'+$ etc. stehen wird. Wir werden weiter unten in §. 114 zeigen, dass dieser Fall die Auflösung der unbestimmten Gleichungen vom ersten Grade mit einschliesst.

X. Ist endlich die Determinante D negativ; so sind in der Kombination $K(m)$ *komb.* $K'(m')$ für m und m' die höchsten Zeiger zu nehmen, bei welchen Übereinstimmung zwischen K und K' stattfindet. Jeder Werth von K' kann auch hier höchstens Eine Auflösung liefern (§. 73), sodass die Anzahl der Auflösungen in diesem Falle eine endliche ist.

XI. In allen diesen Fällen ist noch zu beachten, dass man bei der Reduktion eines Kettenbruches aus den gegebenen Quotienten auch $N_{-2}=-1$, $M_{-1}=-1$ nehmen kann, wodurch alle Zähler und Nenner das entgegengesetzte Zeichen erhalten. Statt dieser neuen Rechnung kann man aber einfach die durch vorstehendes Verfahren gefundenen Auflösungen sämmtlich noch einmal mit entgegengesetzten Zeichen nehmen, sodass man neben der Auflösung x, y auch die Auflösung $-x$, $-y$ erhält.

Wäre $P_0=b=0$, also das in xy multiplizirte Glied nicht vorhanden; so könnte man sogar die Werthe von x für sich und die Werthe von y für sich mit entgegengesetzten Zeichen nehmen, was die Auflösungen x, y; $-x, -y$; $x, -y$; $-x, y$ ergibt.

XII. Durch die bis jetzt beschriebene Rechnung stellen sich die relativ primen Auflösungen heraus. Was die Auflösungen mit einem gemeinschaftlichen Maasse α in der Form $x=\alpha x'$, $y=\alpha y'$ betrifft, worin α verschieden von ± 1 ist; so muss, damit solche Auflösungen überhaupt denkbar sind, die konstante rechte Seite der Gl. (1) den quadratischen Faktor α^2 enthalten, welcher verschieden von 1 ist. Es muss also $k=\alpha^2 k'$ sein.

Besitzt also k einen quadratischen Faktor α^2; so sondert man denselben zu vorstehendem Zwecke ab, und behandelt die Gl.

$$(16) \qquad ax'^2-2bx'y'-cy'^2=k'$$

nach den früheren Regeln, indem man die relativ primen Werthe für x', y' aufsucht und schliesslich $x=\alpha x'$, $y=\alpha y'$ setzt.

Wenn die Determinante positiv und kein Quadrat ist, braucht man nicht erst alle Auflösungen x', y' der Gl. (16) zu suchen und jede mit α zu multipliziren. Man hat vielmehr nur nöthig, wenn man nach §. 84 verfährt, die zu der dortigen Rekursionsformel erforderlichen ersten beiden Auflösungen x', y' zu suchen, eine

jede mit α zu multipliziren und sodann auf die ersten beiden Werthe von $x = \alpha x'$ und $y = \alpha y'$ die betreffende Rekursionsformel in Anwendung zu bringen.

Hierdurch ergeben sich alle Auflösungen, welche Ein und dasselbe gemeinschaftliche Maass α besitzen. Dieselben können übrigens ebenfalls noch mit entgegengesetzten Zeichen genommen werden, wenn man nicht schon vorher die relativ primen Auflösungen für x', y' mit entgegengesetzten Zeichen genommen hat. Um nun alle Auflösungen mit den verschiedenen möglichen gemeinschaftlichen Maassen α, β, γ... zu erhalten, muss man alle verschiedenen quadratischen Faktoren α^2, β^2, γ^2... welche sich einzeln von k absondern lassen, den Einen nach dem anderen absondern und darauf nach obiger Vorschrift verfahren.

Wäre also der grösste quadratische Faktor von k, wenn α, β, γ... gleiche und verschiedene Primzahlen sind, $= (\alpha\beta\gamma\ldots)^2$; so hätte man als gemeinschaftliches Maass von x, y nach und nach die Werthe α, β, γ, $\alpha\beta$, $\alpha\gamma$, $\beta\gamma$, $\alpha\beta\gamma$... anzunehmen, also nach und nach von k die quadratischen Faktoren α^2, β^2, γ^2, $(\alpha\beta)^2$, $(\alpha\gamma)^2$, $(\beta\gamma)^2$, $(\alpha\beta\gamma)^2$... abzusondern.

Diese Absonderung setzt voraus, dass man im Stande sei, eine gegebene Zahl k in ihre Faktoren zu zerlegen. Solches kann durch das mechanische Hülfsmittel einer Faktorentafel geschehen. Streng genommen, besteht jedoch hierin ein wahrhaftes Problem der unbestimmten Analytik, welches man nach §. 113 (s. auch §. 120) lösen kann.

Es wird noch bemerkt, dass wenn $k = 0$ ist, jede beliebige Zahl, also auch jedes Quadrat α^2 als ein Faktor von k angesehen werden kann, sodass jede gefundene Auflösung x, y noch mit der willkürlichen Zahl α multiplizirt werden kann. Ausserdem ist es in diesem Falle kein Erforderniss mehr, dass die Zeigersumme $m + m'$ aus den übereinstimmenden Gliedern von K und K' paar sei, weil $+0 = -0$ zu achten ist.

Wir machen noch darauf aufmerksam, dass es unter Umständen keine Auflösungen in relativ primen Zahlen, gleichwol aber deren mit einem gemeinschaftlichen Maasse geben kann.

XIII. Endlich ist zu bemerken, dass es mit Rücksicht auf möglichste Ökonomie der Rechnung in den meisten Fällen rathsam ist, diejenige Unbekannte mit x zu bezeichnen und in das erste Glied der aufzulösenden Gleichung zu stellen, deren Quadrat mit dem numerisch kleineren Koeffizienten behaftet ist.

Anderweite wichtige Bemerkungen für die Fälle, wo die Determinante D ein Quadrat oder null ist, findet man in §. 107 ff.

§. 101. **Beispiel mit positiver nicht quadratischer Determinante:**

$$7x^2 - 18xy + 10y^2 = 7$$

Hier hat man $a = 7$, $b = 9$, $c = -10$ also $D = b^2 + ac = 9^2 + 7(-10) = 11$ und $K = \frac{\sqrt{11} + 9}{7}$, wovon die Entwickelung folgende ist.

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-10		1	0
0	9	7	1	1	1
1	-2	1	1	2	1
2	3	2	3	7	4
3	3	1	6	44	25
4	3	2	3	139	79
5	3	1	6	878	499

Um nun die Grösse $K' = \frac{\sqrt{D} + p}{k}$ zu bilden, hat man $D = 11$, $k = 7$. Sucht man die verschiedenen Reihen der durch 7 theilbaren Zahlen von der Form $J = 11 - p^2$ so findet man $p = \pm 2$.

Nimmt man erst $K' = \frac{\sqrt{11} + 2}{7}$ so gibt Dies die Entwikkelung

n	P'_n	Q'_n	a'_n
-1		1	
0	2	7	0
1	-2	1	1
2	3	2	3
3	3	1	6
4	3	2	3
5	3	1	6

Die Periode von K', welche $r = 2$ Glieder besitzt, stimmt mit der von K überein, und zwar immer bei Zeigern m und m', deren Summe $m + m'$ eine paare Zahl ist. Die Kombinationen Beider nach den Formeln

$K(2)$, (4), (6), (8) . . . *komb.* $K'(2)$

$K(2)$ *komb.* $K'(2)$, (4), (6), (8) . . .

müssen also lauter Auflösungen ergeben.

Um dieselben nach der Rekursionsformel des §. 84 zu berechnen, so hat man für die ersten beiden Kombinationen

$K(2)$ *komb.* $K'(2)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	0	1	1
3	-1	1	0

$K(4)$ *komb.* $K'(2)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	3	7	4
3	6	44	25
4	0	7	4
5	-1	37	21

also

$$\overset{0}{M}=1,\ \overset{0}{N}=0, \qquad \overset{1}{M}=37,\ \overset{1}{N}=21$$

Der Werth von $h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}$ nach §. 82 und 84 findet sich aus der Periode von K durch die Berechnung von $\mathfrak{K}_{r-1}=[a_m, a_{m+1}\ldots a_{m+r-1}]=[a_2, a_3]=[3, 6]$. Dies gibt

	n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
	-2		0	1
	-1		1	0
	0	3	3	1
$r-1=$	1	6	19	6

Hiernach ist $h=19+1=20$ und da $r=2$ ist; so erhält man für die Rekursionsformeln (19) und (20) in §. 84

$$\overset{n}{M}=20\overset{n-1}{M}-\overset{n-2}{M} \qquad \overset{n}{N}=20\overset{n-1}{N}-\overset{n-2}{N}$$

$$\overset{n}{M}=20\overset{n+1}{M}-\overset{n+2}{M} \qquad \overset{n}{N}=20\overset{n+1}{N}-\overset{n+2}{N}$$

wovon die oberen Formeln den Kombinationen $K(2)$, (4), (6)... *komb.* $K'(2)$ und die unteren den Kombinationen $K(2)$ *komb.* K' (2), (4), (6)... entsprechen.

Im Zusammenhange hat man für Beide folgende nach beiden Seiten ins Unendliche fortlaufende Reihe von Auflösungen

n	h	$\overset{n}{M}=x$	$\overset{n}{N}=y$
-5	20	-2707577	-3334821
-4	20	-135719	-167160
-3	20	-6803	-8379
-2	20	-341	-420
-1	20	-17	-21
0	20	1	0
1	20	37	21
2	20	739	420
3	20	14743	8379
4	20	294121	167160
5	20	5867677	3334821

Jede zwei zusammengehörige Werthe von $\overset{n}{M}$, $\overset{n}{N}$ bilden eine Auflösung x, y der gegebenen Gleichung. Dieselben ordnen sich von der Mitte heraus nach ihrer numerischen Grösse, und können auch mit entgegengesetzten Zeichen genommen werden.

Um fernere Auflösungen zu finden, hat man hier, wo die Periode von K symmetrisch ist, auch den zweiten Werth von K', welcher $\frac{\sqrt{11}-2}{7}$ ist, zu entwickeln. Dies gibt

n	P'_n	Q'_n	a'_n
-1		1	
0	-2	7	0
1	2	1	5
⎧2	3	2	3
⎩3	3	1	6
⎧4	3	2	3
⎩5	3	1	6

Derselbe kann ebenso wie der vorhergehende Werth von K' mit K kombinirt werden. Dies gibt für die ersten beiden Kombinationen

$K(2)$ *komb.* $K'(2)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	0	1	1
3	-5	-3	-4

$K(4)$ *komb.* $K'(2)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	3	7	4
3	6	44	25
4	0	7	4
5	-5	9	5

also

$$\overset{0}{M} = -3, \quad \overset{0}{N} = -4 \qquad\qquad \overset{1}{M} = 9, \quad \overset{1}{N} = 5$$

Da h denselben Werth 20 behält und die früheren Rekursionsformeln gelten; so erhält man folgende neue Reihe von Auflösungen

n	h	$\overset{n}{M} = x$	$\overset{n}{N} = y$
-3	20	-27471	-33835
-2	20	-1377	-1696
-1	20	-69	-85
0	20	-3	-4
1	20	9	5
2	20	183	104
3	20	3651	2075
4	20	72837	41396

Auch diese Auflösungen können mit entgegengesetzten Zeichen genommen werden.

Ausser den gefundenen beiden Reihen von Auflösungen und den entgegengesetzten Werthen derselben kann es keine in relativ primen Zahlen geben. Auflösungen mit gemeinschaftlichem Maasse sind übrigens hier unmöglich, weil $k = 7$ keinen quadratischen Faktor enthält.

§. 102. *Beispiel mit positiver nicht quadratischer Determinante:*

$$7x^2 - 18xy + 10y^2 = 3$$

Die linke Seite dieser Gleichung ist dieselbe wie im vorhergehenden Beispiele; es hat also K den früheren Werth $\frac{\sqrt{11} + 9}{7}$. Die rechte Seite aber ist $k = 3$. Es sind also zur Darstellung von K' die durch 3 theilbaren Zahlen J von der Form $11 - p^2$ zu suchen. Da es deren nicht gibt; so ist die Auflösung in relativ primen Zahlen unmöglich. Da $k = 3$ keinen quadratischen Faktor besitzt; so gibt es auch keine Auflösungen mit gemeinschaftlichem Maasse.

Wäre dagegen die Gleichung

$$7x^2 - 18xy + 10y^2 = 63$$

gegeben; so gibt es zwar keine Auflösungen in relativ primen Zahlen, weil es keine durch 3, mithin auch keine durch 63 theilbare Zahl von der Form $11-p^2$ gibt: es sind jedoch, weil $63=3^2.7=\alpha^2 k'$ den quadratischen Faktor 3^2 enthält, und für $k'=7$ die Gleichung

$$7x'^2-18x'y'+10y'^2=7$$

alle im vorhergehenden Paragraphen gefundenen Auflösungen besitzt, Auflösungen mit dem gemeinschaftlichen Maasse $\alpha=3$ vorhanden. Die Letzteren werden erhalten, wenn man die Auflösungen aus §. 101 mit 3 multiplizirt.

§. 103. *Beispiel mit positiver nicht quadratischer Determinante:*

$$-3x^2-8xy+7y^2=-3$$

Hier ist $a=-3$, $b=4$, $c=-7$ also $D=b^2+ac$ $=4^2+(-3)(-7)=37$ und $K=\frac{\sqrt{37}+4}{-3}$. Dies gibt die Entwickelung

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-7		1	0
0	4	-3	-4	-4	1
1	8	9	1	-3	1
2	1	4	1	-7	2
3	3	7	1	-10	3
4	4	3	3	-37	11
5	5	4	2	-84	25
6	3	7	1	-121	36
7	4	3	3	-447	133
8	5	4	2	-1015	302

Da in dieser Entwickelung unter den Grössen $(-1)^n Q_n$ der Werth von $k=-3$, nämlich bei dem Zeiger 0 und ausserdem in den Perioden bei den Zeigern 7, 13, 19 . . . vorkommt; so liefert Dies sofort schon die Auflösungen

$$x=1,\ -121\ \ldots$$
$$y=0,\ \ \ 36\ \ldots$$

Wir können jedoch diese Auflösungen ganz ausser Acht lassen, da sich dieselben bei den Kombinationen von K und K' wiederholen müssen.

Jetzt sind, da $k=-3$ ist, die Reihen der durch 3 theilbaren Zahlen J von der Form $37-p^2$ aufzusuchen. Es finden sich deren zwei, für welche $p=\pm 1$ ist. Nimmt man erst den Werth $p=1$; so hat man $K'=\frac{\sqrt{37}+1}{-3}$, also

n	P'_n	Q'_n	a'_n
-1		-12	
0	1	-3	-3
1	8	9	1
2	1	4	1
3	3	7	1
4	4	3	3
5	5	4	2
6	3	7	1

Die dreigliedrige Periode von K' stimmt mit der von K überein, und da dieselbe eine unpaare Gliederzahl besitzt; so sind jedenfalls Auflösungen vorhanden. Man hat hier jedoch aus bekannten Gründen, damit $m+m'$ paar sei, die Periode von doppelter Länge, also $r=6$ zu nehmen, was der Periode der Grössen $(-1)^n Q_n$ entspricht.

Hiernach kann man in folgender Weise kombiniren:

$$K(3),\ (9),\ (15),\ (21)\ldots\ komb.\ K'(3)$$

$$K(3)\ komb.\ K'(3),\ (9),\ (15),\ (21)\ldots$$

Mit Bezug auf die schon in der Entwickelung von K berechneten Zähler und Nenner der Näherungsbrüche hat man für die ersten beiden Kombinationen

$K(3)$ *komb.* $K'(3)$

n	a_n	M_n	N_n
1		-3	1
2		-7	2
3	0	-3	1
4	-1	-4	1
5	-1	1	0

$K(9)$ *komb.* $K'(3)$

n	a_n	M_n	N_n
7		-447	133
8		-1015	302
9	0	-447	133
10	-1	-568	169
11	-1	121	-36

also $\overset{0}{M}=1,\ \overset{0}{N}=0$ $\qquad \overset{1}{M}=121,\ \overset{1}{N}=-36$

Zur Berechnung von $h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}$ aus $\mathfrak{K}_{r-1}=[1,3,2,1,3,2]$ hat man

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	1	1	1
1	3	4	3
2	2	9	7
3	1	13	10
4	3	48	37
$r-1=5$	2	109	84

also $h=109+37=146$ und mithin

$$\overset{n}{M}=146\,\overset{n-1}{M}-\overset{n-2}{M} \qquad \overset{n}{N}=146\,\overset{n-1}{N}-\overset{n-2}{N}$$

$$\overset{n}{M}=146\,\overset{n+1}{M}-\overset{n+2}{M} \qquad \overset{n}{N}=146\,\overset{n+1}{N}-\overset{n+2}{N}$$

Im Zusammenhange ergeben diese beiden Rekursionsformeln folgende Reihe von Auflösungen

n	h	$\overset{n}{M}=x$	$\overset{n}{N}=y$
-2	146	3649	5256
-1	146	25	36
0	146	1	0
1	146	121	-36
2	146	17765	-5256

welche auch noch mit entgegengesetzten Zeichen genommen werden können.

Da die Periode des vorstehenden Werthes von K' für $p=+1$ nicht symmetrisch ist; so kann, nachdem dieser Werth von K' als ein zulässiger befunden worden, der Werth von K' für $p=-1$ kein brauchbarer sein.

Auflösungen mit gemeinschaftlichem Maasse sind hier nicht möglich, da $k=-3$ keinen quadratischen Faktor enthält.

§. 104. Beispiel mit positiver nicht quadratischer Determinante:

$$x^2 - 3xy - 2y^2 = 4$$

Da hier der Koeffizient des in xy multiplizirten Gliedes eine unpaare Zahl ist; so muss die Gleichung, ehe sie weiter behandelt werden kann, mit 2 multiplizirt werden. Dies gibt die Gleichung

$$2x^2 - 6xy - 4y^2 = 8.$$

Hierin ist $a=2$, $b=3$, $c=4$, also $D=b^2+ac=3^2+2.4=17$ und $K=\frac{\sqrt{17}+3}{2}$. Dies gibt

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		4		1	0
0	3	2	3	3	1
1	3	4	1	4	1
2	1	4	1	7	2
3	3	2	3	25	7
4	3	4	1	32	9
5	1	4	1	57	16

Jetzt sind die Reihen der durch $k=8$ theilbaren Zahlen J von der Form $17-p^2$ aufzusuchen. Es gibt deren vier, für welche man $p=\pm 1, \pm 3$ hat. Der erste Werth von K' ist also $=\frac{\sqrt{17}+1}{8}$ und gibt die Entwickelung

n	P'_n	Q'_n	a'_n
-1		2	
0	1	8	0
1	-1	2	1
2	3	4	1
3	1	4	1
4	3	2	3
5	3	4	1
6	1	4	1

Die dreigliedrige Periode von K' stimmt mit der von K überein. Da dieselbe eine unpaare Gliederzahl besitzt; so ist sie doppelt, also $r = 6$ zu nehmen, und man kann folgendermaassen kombiniren:

K (0), (6), (12), (18)... *komb.* K' (4)

K (0) *komb.* K' (4), (10), (16), (22)...

Zunächst hat man für die ersten beiden Kombinationen

K (0) *komb.* K' (4)

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	-1	1	-1
2	-1	-1	2
3	-1	2	-3

K (6) *komb.* K' (4)

n	a_n	M_n	N_n
4		32	9
5		57	16
6	0	32	9
7	-1	25	7
8	-1	7	2
9	-1	18	5

also $\overset{0}{M} = 2$, $\overset{0}{N} = -3$ $\quad$ $\overset{1}{M} = 18$, $\overset{1}{N} = 5$

Der Werth von $h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2}$ ergibt sich aus

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	3	3	1
1	1	4	1
2	1	7	2
3	3	25	7
4	1	32	9
$r - 1 = 5$	1	57	16

und man hat $h = 57 + 9 = 66$.

Hieraus ergibt sich folgende Reihe von Auflösungen.

n	h	$\overset{n}{M} = x$	$\overset{n}{N} = y$
-1	66	114	-203
0	66	2	-3
1	66	18	5
2	66	1186	333

Da die Entwickelung von K' eine symmetrische dreigliederige Periode enthält (welche bei dem Zeiger 2 beginnt) so ist ausser dem vorstehenden Werthe von K' für $p = 1$ auch noch der zweite Werth von K' für $p = -1$, also der Werth $\frac{\sqrt{17} - 1}{8}$ zu betrachten. Man findet, dass dieser Werth in der That eine neue Reihe von Auflösungen liefert.

Was die übrigen beiden Werthe von K' betrifft, welche in der Form $\frac{\sqrt{17} \pm 3}{8}$ enthalten sind; so findet man, dass deren Periode nicht mit der von K übereinstimmt. Aus diesen Werthen von K' ergeben sich also keine weiteren Auflösungen.

Dagegen kann man hier, wo $k = 8 = 2^2 . 2$ ist, nach Auflösungen mit dem gemeinschaftlichen Maasse $\alpha = 2$ fragen.

Behandelt man demzufolge die Gleichung

$$2x'^2 - 6x'y' - 4y'^2 = 2$$

so sind die Reihen der durch 2 theilbaren Zahlen von der Form $17 - p^2$ zu suchen. Die zwei für $p = \pm 1$ sich ergebenden konjugirten Reihen sind identisch; man hat es also nur mit einer einzigen, und demnach auch nur mit dem einzigen Werthe $K' = \frac{\sqrt{17}+1}{2}$ zu thun. Derselbe ergibt

n	P'_n	Q'_n	a'_n
-1		8	
0	1	2	2
1	3	4	1
2	1	4	1
3	3	2	3
4	3	4	1
5	1	4	1

Diese Periode von K' stimmt mit der von K überein. Man thut jedoch jetzt besser, die Perioden von K und K' von den Zeigern $m = 1$, $m' = 1$ an zu rechnen, indem Dies offenbar die leichteste Rechnung ergibt. Demzufolge kann man kombiniren:

K (1), (7), (13), (19) . . . *komb.* K' (1)

K (1) *komb.* K' (1), (7), (13), (19) . . .

Nun hat man für die ersten beiden Kombinationen

K (1) *komb.* K' (1)

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	3	3	1
1	0	1	0

K (7) *komb.* K' (1)

n	a_n	M_n	N_n
4		32	9
5		57	16
6	3	203	57
7	0	57	16

also $\overset{0}{M} = 1$, $\overset{0}{N} = 0$ $\qquad \overset{1}{M} = 57$, $\overset{1}{N} = 16$

Multiplizirt man diese beiden speziellen Auflösungen für x', y' mit 2; so erhält man sofort die beiden korrespondirenden Auflösungen für x, y, welche also sind

$$\overset{0}{M} = 2,\ \overset{0}{N} = 0 \qquad \overset{1}{M} = 114,\ \overset{1}{N} = 32$$

Um dieselben der Rekursionsformel in §. 84 unterzulegen, hat man zur Berechnung von $h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2}$

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	3	7	4
3	1	9	5
4	1	16	9
$r - 1 = 5$	3	57	32

also $h = 57 + 9 = 66$. Hiernach erhält man folgende Reihe von Auflösungen

n	h	$\overset{n}{M}=x$	$\overset{n}{N}=y$
-2	66	1186	-2112
-1	66	18	-32
0	66	2	0
1	66	114	32
2	66	7522	2112

welche noch mit entgegengesetzten Zeichen genommen werden kann.

§. 105. *Beispiel mit positiver nicht quadratischer Determinante:*

$$5x^2 - 2xy - 2y^2 = 1$$

Hier ist $a=5$, $b=1$, $c=2$, also $D=b^2+ac=1+5.2=11$ und $K=\frac{\sqrt{11}+1}{2}$. Dies gibt

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		2		1	0
0	1	5	0	0	1
1	-1	2	1	1	1
(2	3	1	6	6	7
3)	3	2	3	19	22
(4	3	1	6	120	139
5)	3	2	3	379	439

Da hier $k=1$ ist; so gibt es nur Eine Reihe der durch 1 theilbaren Zahlen von der Form $11-p^2$, nämlich diejenige symmetrische, für welche $p=0$ ist. Dies gibt $K'=\frac{\sqrt{11}+0}{1}$, also

n	P'_n	Q'_n	a'_n
-1		11	
0	0	1	3
1	3	2	3
(2	3	1	6
3)	3	2	3

Die Periode von K' stimmt mit der von K so überein, dass man die Kombinationen

$K(2)$, (4), (6), (8) ... *komb.* K' (2)

$K(2)$ *komb.* K' (2), (4), (6), (8) ...

bilden kann. Nun hat man für die ersten beiden Kombinationen

$K(2)$ *komb.* K' (2)

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	0	0	1
3	-3	1	-2

also $\overset{0}{M}=1$, $\overset{0}{N}=-2$

$K(4)$ *komb.* K' (2)

n	a_n	M_n	N_n
2		6	7
3		19	22
4	0	6	7
5	-3	1	1

$\overset{1}{M}=1$, $\overset{1}{N}=1$

Der Werth von $h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2}$ findet sich durch

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	6	6	1
$r-1=1$	3	19	3

und ist $h = 19 + 1 = 20$. Dies gibt folgende Reihe von Auflösungen

n	h	$\overset{n}{M} = x$	$\overset{n}{N} = y$
-3	20	7561	-16319
-2	20	379	-818
-1	20	19	-41
0	20	1	-2
1	20	1	1
2	20	19	22
3	20	379	439
4	20	7561	8758

Ausser diesen und den direkt entgegengesetzten gibt es keine Auflösungen.

§. 106. ***Beispiel mit positiver nicht quadratischer Determinante:***

$$5x^2 - 3y^2 = 3$$

Hier ist $a = 5$, $b = 0$, $c = 3$, also $D = b^2 + ac = 5.3 = 15$ und $K = \frac{\sqrt{15} + 0}{5}$, mithin

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		3		1	0
0	0	5	0	0	1
1	0	3	1	1	1
2	3	2	3	3	4
3	3	3	2	7	9
4	3	2	3	24	31
5	3	3	2	55	71

Es gibt nur Eine symmetrische Reihe der durch $k = 3$ theilbaren Zahlen J von der Form $15 - p^2$, für welche $p = 0$ ist. Dies gibt $K' = \frac{\sqrt{15} + 0}{3}$

n	P'_n	Q'_n	a'_n
-1		5	
0	0	3	1
1	3	2	3
2	3	3	2

Die zweigliedrige Periode von K' stimmt zwar mit der von K überein, aber immer bei Zeigern, für welche die Summe $m + m'$ eine unpaare Zahl ist. Hieraus folgt, dass die Kombinationen zwischen K und K', wie z. B. $K(2)$ *komb.* K' (1), zu keinen Auflösungen führen können. Die Aufgabe ist also unmöglich.

Wäre dagegen die Gleichung

$$5x^2 - 3y^2 = -3$$

gegeben; so gäbe es für K' auch nur einen einzigen Werth $K' = \frac{\sqrt{15}+0}{-3}$. Derselbe führt aber zu der Entwickelung

n	P_n	Q_n	a_n
-1		-5	
0	0	-3	-2
1	6	7	1
2	1	2	2
3	3	3	2
(4	3	2	3
5)	3	3	2

Die Periode von K' stimmt jetzt so mit der von K überein, dass die Zeigersumme $m + m'$ paar ist, also Auflösungen zu erwarten sind. Man kann kombiniren:

K (2), (4), (6), (8) . . . *komb.* K' (4)

K (2) *komb.* K' (4), (6), (8), (10) . . .

Für die ersten beiden Kombinationen hat man

K (2) *komb.* K' (4)

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	0	0	1
3	-2	1	-1
4	-2	-2	3
5	-1	3	-4

K (4) *komb.* K' (4)

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	3	3	4
3	2	7	9
4	0	3	4
5	-2	1	1
6	-2	1	2
7	-1	0	-1

also $\overset{0}{M} = 3$, $\overset{0}{N} = -4$ $\qquad$ $\overset{1}{M} = 0$, $\overset{1}{N} = -1$

Zur Bestimmung von $h = \mathfrak{M}_{r-1} + \mathfrak{N}_{r-2}$ hat man

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	3	3	1
$r-1=1$	2	7	2

also $h = 7 + 1 = 8$, und Dies ergibt folgende Reihe von Auflösungen

n	h	$\overset{n}{M} = x$	$\overset{n}{N} = y$
-3	8	1488	-1921
-2	8	189	-244
-1	8	24	-31
0	8	3	-4
1	8	0	-1
2	8	-3	-4
3	8	-24	-31
4	8	-189	-244
5	8	-1488	-1921

welche auch noch mit entgegengesetzten Zeichen genommen werden können.

§. 107. ***Beispiel mit quadratischer Determinante:***

$$5x^2 + 8xy - 4y^2 = 5$$

Hier ist $a = 5$, $b = -4$, $c = 4$, also $D = b^2 + ac = (-4)^2 + 5.4 = 36 = 6^2$ und $K = \frac{\sqrt{36} - 4}{5}$. Die Entwickelung hiervon ist

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		4		1	0
0	-4	5	0	0	1
1	4	4	2	1	2
2	4	5	2	2	5
3	6	0			

Da der vorletzte Werth von Q, nämlich $Q_2 = 5$, positiv und $< \sqrt{36}$ ist; so liegt ein Schluss in kleinsten positiven Zahlen vor.

Nun sind die Reihen der durch $k = 5$ theilbaren Zahlen J von der Form $36 - p^2$ zu suchen. Es gibt deren zwei für $p = \pm 1$. Für den ersten Werth $p = 1$ hat man $K' = \frac{\sqrt{36} + 1}{5}$ also

n	P'_n	Q'_n	a'_n
-1		7	
0	1	5	
1	4	4	1
2	4	5	2
3	6	0	2

Dies ist ebenfalls ein Schluss in kleinsten positiven Zahlen, welcher mit dem von K so übereinstimmt, dass die Zeigersumme $m + m'$ paar ist. Demnach erhält man durch die Kombination

$$K(1) \; komb. \; K'(1)$$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	0	1	0

die Auflösung

$$x = 1, \quad y = 0$$

welche auch mit entgegengesetzten Zeichen genommen werden kann.

Der zweite Werth von K', nämlich $\frac{\sqrt{36} - 1}{5}$ gibt

n	P_n	Q_n	a_n
-1		7	
0	-1	5	1
1	6	0	

Dies ist ebenfalls ein mit dem von K übereinstimmender Schluss in kleinsten positiven Zahlen, für welchen die Zeigersumme $m + m'$ paar ist. Demnach führt die Kombination

$K(3)$ *komb.* $K'(1)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	2	1	2
2	2	2	5
3	0	1	2

zu der zweiten Auflösung

$$x = 1, \quad y = 2$$

welche ebenfalls mit entgegengesetzten Zeichen genommen werden kann.

Da $k = 5$ keinen quadratischen Faktor besitzt; so kann es Auflösungen mit gemeinschaftlichem Maasse nicht geben, und die vorhin gefundenen sind die einzig möglichen.

§. 108. ***Beispiel mit quadratischer Determinante:***

$$5x^2 + 8xy - 4y^2 = 0$$

Die linke Seite dieser Gleichung stimmt mit der im vorhergehenden Paragraphen betrachteten überein. Indem wir uns also auf den Anfang der dortigen Entwickelung beziehen, haben wir $K = \frac{\sqrt{36} - 4}{5}$.

Die rechte Seite k der gegenwärtigen Gleichung ist $= 0$. Dies veranlasst uns zuvörderst zu einer allgemeinen Bemerkung über die Gleichung

$$ax^2 - 2bxy - cy^2 = 0.$$

Es ist klar, dass eine solche Gleichung, wenn die Determinante $D = b^2 + ac$ positiv und kein Quadrat, oder wenn sie negativ ist, in relativ primen Zahlen unlösbar ist, indem unter solchen Umständen der Werth 0 in der Reihe der bei den Kettenbruchsentwickelungen auftretenden Grössen Q niemals erscheinen kann.

Wol aber ist jene Gleichung in relativ primen Zahlen dann stets lösbar, wenn die Determinante ein Quadrat ist.

Dagegen hat jene Gleichung in dem zuerst genannten Falle stets Eine, aber auch nur Eine Auflösung mit gemeinschaftlichem Maasse null. Dieselbe ist $x = 0$, $y = 0$ und ergibt sich im Sinne unserer Methode, wenn man die rechte Seite der gegebenen Gleichung als mit dem quadratischen Faktor 0^2 und irgend einem anderen w behaftet ansieht, oder $k = 0 = 0^2 w$ setzt. Nun ist klar, dass es für w Werthe geben muss, bei welchen die Gleichung $ax'^2 - 2bx'y' - cy'^2 = w$ lösbar wird. Welches aber auch diese Auflösungen x', y' seien,

immer wird $x = 0 . x' = 0$ und $y = 0 . y' = 0$ sein. Dächte man sich k als aus einem beliebigen quadratischen Faktor w^2 und 0 bestehend, also $k = 0 = w^2 . 0$; so würde die Absonderung von w^2 die ursprüngliche, in relativ primen Zahlen unlösbare Gleichung wiedererzeugen. Es kann also ausser der Auflösung $x = 0$, $y = 0$ keine andere Auflösung mit gemeinschaftlichem Maasse geben.

Wol aber gibt es, wenn die Determinante ein Quadrat ist, stets noch Auflösungen mit gemeinschaftlichem Maasse. Um dieselben darzustellen, denkt man sich $k = 0 = w^2 . 0$ gesetzt. Alle Auflösungen der gegebenen Gleichung sind offenbar auch Auflösungen der durch Absonderung von w^2 entstehenden Gleichung $ax'^2 - 2bx'y' - cy'^2 = 0$. Multiplizirt man nun eine jede mit w; so ergeben sich die neuen Auflösungen in der Form $x = wx'$, $y = wy'$. Man kann also jede Auflösung in relativ primen Zahlen, deren Anzahl stets endlich sein wird, mit einer willkürlichen ganzen Zahl w multipliziren. Hierdurch ergeben sich eine unendliche Menge Auflösungen mit gemeinschaftlichem Maasse.

Setzen wir nun die Auflösung der oben gegebenen speziellen Gleichung fort; so sind die Reihen der durch $k = 0$ theilbaren Zahlen J von der Form $36 - p^2$ zu suchen. Für diesen Werth von k kommen nur die beiden Werthe $p = \pm 6$ in Betracht. Man hat also zunächst $K' = \frac{\sqrt{36} + 6}{0}$.

Nach §. 91 weiss man, dass die Entwickelung dieses Ausdruckes mit dem ersten Zeiger schon geschlossen ist, und dass für die Grösse Q'_{-1}, welche hier durch Nichts näher bestimmt ist, weil es immer nur auf einen Schluss in kleinsten positiven Zahlen ankommt, nach und nach die sieben Werthe 0, 1, 2, 3, 4, 5, 6 zu setzen sind. Hiervon ist es jedoch nur die Zahl 5, welche den Schluss von K' mit dem von K in Übereinstimmung zu bringen vermag. Man hat also

n	P'_n	Q'_n	a'_n
-1		5	
0	6	0	

In der Kombination $K(3)$ *komb.* $K'(0)$ ist zwar die Zeigersumme $m + m' = 3 + 0 = 3$ unpaar; Dies ist jedoch für $k = 0$ vollkommen erlaubt. Da $K(3)$ *komb.* $K'(0) = K(3)$ ist; so liefert Dies die Auflösung $x = M_2 = 2$, $y = N_2 = 5$.

Der zweite Werth von K' ist $\frac{\sqrt{36} - 6}{0}$. Auch für diesen ist Q'_{-1} völlig unbestimmt, und demzufolge nach §. 91 sukzessive $= 0, 1, 2, 3, 4, 5, 6$ anzunehmen. Hierunter muss nothwendig Ein, aber auch nur Ein Werth sein, welcher den Schluss

von K' in kleinsten positiven Zahlen mit dem von K in Übereinstimmung bringt. Man findet, dass Dies der Werth $Q_{-1} = 5$ ist, indem man dafür

n	P'_n	Q'_n	a'_n
-1		5	
0	-6	0	0
1	6	5	2
2	4	4	2
3	4	5	2
4	6	0	

hat. Bildet man hiernach $K(1)$ *komb.* $K'(2)$; so kommt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	0	1	0
2	-2	-2	1

also die zweite Auflösung $x = -2$, $y = 1$.

Ausser diesen beiden Auflösungen in relativ primen Zahlen hat man unendlich viele mit gemeinschaftlichem Maasse. Alle diese und jene sind in den Formeln

$$x = 2w = \ldots -6, \; -4, \; -2, \; 0, \; 2, \; 4, \; 6 \ldots$$
$$y = 5w = \ldots -15, \; -10, \; -5, \; 0, \; 5, \; 10, \; 15 \ldots$$

und

$$x = -2w = \ldots \; 6, \; 4, \; 2, \; 0, \; -2, \; -4, \; -6 \ldots$$
$$y = \; w = \ldots -3, \; -2, \; -1, \; 0, \; 1, \; 2, \; 3 \ldots$$

enthalten.

§. 109. ***Beispiel mit quadratischer Determinante:***

$$9x^2 - 20xy + 11y^2 = -8$$

Hier ist $a = 9$, $b = 10$, $c = -11$, also $D = b^2 + ac = 10^2 + 9(-11) = 1$ und $K = \frac{\sqrt{1} + 10}{9}$, folglich

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-11		1	0
0	10	9	1	1	1
1	-1	0	4	5	4
2	1	1	2	11	9
3	1	0			

In dieser Entwickelung stösst man bei dem Zeiger 1 auf den Ausdruck $x_1 = \frac{\sqrt{1} - 1}{0}$, welcher nach §. 87 in vorstehender Weise weiterentwickelt und zum Schlusse geführt wird. Der sich ergebende Schluss ist offenbar Einer in kleinsten positiven Zahlen.

Jetst sind die Reihen der durch $k = -8$ theilbaren Zahlen von der Form $1 - p^2$ aufzusuchen. Es gibt deren vier resp. für $p = \pm 1, \pm 3$.

Der erste Werth für K' ist also $=\frac{\sqrt{1}+1}{-8}$ und ergibt

n	P'_n	Q'_n	a'_n
-1		0	
0	1	-8	-1
1	7	6	1
2	-1	0	3
3	1	0	

Dieser Schluss, welcher Einer in kleinsten positiven Zahlen ist, stimmt mit dem von K nicht überein, weshalb die Kombination K mit diesem K' zu keiner Auflösung führt.

Der zweite Werth $\frac{\sqrt{1}-1}{-8}$ von K' ist nach §. 91 zu entwickeln, indem man beachtet, dass hierin der Werth von $Q'_{-1}=\frac{1-(-1)^2}{-8}=0$ vollkommen bestimmt ist. Dies gibt

n	P'_n	Q'_n	a'_n
-1		0	
0	-1	-8	0
1	1	0	

Der Schluss dieser Entwickelung ist keiner in kleinsten positiven Zahlen. Um einen solchen zu erhalten, hat man nach §. 90 zu verfahren, also mit $2.1=2$ in $Q'_0=-8$ zu dividiren. Dies gibt statt der dortigen Formel (1) oder (2)
$Q_{n-1}=2aw+R$

$$-8=2.1.(-4)+0 \quad \text{also } R=0$$

Da in dem hierdurch zu erzeugenden Schlusse $R=0$ der Werth des vorletzten Q sein wird; so erhellet, dass dieser Schluss nicht mit dem von K übereinstimmen, also ebenfalls keine Auflösung liefern wird.

Der dritte Werth von K' ist $\frac{\sqrt{1}+3}{-8}$ und gibt

n	P'_n	Q'_n	a'_n
-1		1	
0	3	-8	-1
1	5	3	2
2	1	0	

Diese Entwickelung von K' hat keinen Schluss in kleinsten positiven Zahlen. Um einen solchen zu erzeugen, hat man statt der Gl. (1) in §. 90

$$Q_1=3=2.1.1+1 \quad \text{also } R=1$$

Da hiernach $w=1$ ist; so hat man die vorstehende Entwickelung von K' in der Weise fortzusetzen, dass man $a'_2=-w=-1$ und $a'_3=0$ nimmt. Dies gibt im Zusammenhange nach §. 88

n	P'_n	Q'_n	a'_n
-1		1	
0	3	-8	-1
1	5	3	2
2	1	0	-1
3	-1	1	0
4	1	0	

Dieser Schluss von K' stimmt zwar mit dem von K überein; die Zeigersumme $m + m'$ ist aber $3 + 4 = 7$, also eine unpaare Zahl: mithin lässt sich dieser Werth von K' in der vorstehenden Entwickelung nicht mit K behuf Erzielung einer Auflösung kombiniren. Da aber der vorletzte Werth der Grösse Q im Schlusse dieser Entwickelung $Q_{n-1} = Q_3 = 1$ ein Vielfaches von $\sqrt{D} = \sqrt{1}$ ist; so weiss man aus §. 90, dass derselbe Schluss in einem Abstande von drei Gliedern nochmals reproduzirt werden kann, indem man nach der dortigen Gl. (2)

$$Q_3 = 1 = 2 \,.\, 1 \,.\, 1 - 1 \quad \text{also } R = 1$$

und alsdann, da $w = 1$ ist, nach der dortigen Formel (4) $a_4, a_5, a_6 = -2, 1, -1$ nimmt. Dies gibt nach §. 88 im Zusammenhange.

n	P'_n	Q'_n	a'_n
-1		1	
0	3	-8	-1
1	5	3	2
2	1	0	-1
3	-1	1	0
4	1	0	-2
5	-1	-3	1
6	-2	1	-1
7	1	0	

Jetzt kann man die Kombination $K(3)$ *komb.* $K'(7)$, für welche auch die Zeigersumme $3 + 7 = 10$ eine paare Zahl ist, ausführen. Dies gibt

n	a_n	M_n	N_n
1		5	4
2		11	9
3	0	5	4
4	1	16	13
5	-1	-11	-9
6	2	-6	-5
7	0	-11	-9
8	1	-17	-14
9	-2	23	19

also $x = 23$, $y = 19$.

Der vierte Werth von K' ist $\frac{\sqrt{1} - 3}{-8}$. Die Entwickelung desselben führt bei dem Zeiger 2 zu demselben Schlusse wie die ursprüngliche Entwickelung von $\frac{\sqrt{1} + 3}{-8}$ bei dem Zeiger 4.

Man hat also auch hier denselben Schluss in einem Abstande von drei Gliedern nochmals zu reproduziren. Dies gibt

n	P'_n	Q'_n	a'_n
-1		1	
0	-3	-8	0
1	3	1	4
2	1	0	-2
3	-1	-3	1
4	-2	1	-1
5	1	0	

Kombinirt man jetzt K (3) *komb.* K' (5); so kommt

n	a_n	M_n	N_n
1		5	4
2		11	9
3	0	5	4
4	1	16	13
5	-1	-11	-9
6	2	-6	-5
7	-4	13	11

also $x = 13$, $y = 11$. Diese und die vorhergehende Auflösung, welches die einzigen in relativ primen Zahlen sind, können noch mit entgegengesetzten Zeichen genommen werden.

Es sind nun noch, da $k = -8 = 2^2(-2)$ den quadratischen Faktor 2^2 besitzt, die etwaigen Auflösungen mit dem gemeinschaftlichen Maasse 2 zu untersuchen. Zu diesem Ende hat man für $k' = -2$ die durch 2 theilbaren Zahlenreihen von der Form $1 - p^2$ zu untersuchen. Es gibt deren Eine für $p = 1$, indem die andere für $p = -1$ mit jener identisch ist. Es findet sich jedoch, dass in dem Schlusse in kleinsten positiven Zahlen von $K' = \frac{\sqrt{1}+1}{-2}$ das vorletzte Q den Werth 0 annimmt, dass also dieser Schluss mit dem von K nicht übereinstimmt.

Demnach hat die gegebene Gleichung keine Auflösungen mit einem gemeinschaftlichen Maasse.

§. 110. ***Beispiel mit quadratischer Determinante:***

$$9x^2 - 20xy + 11y^2 = 0.$$

Die linke Seite dieser Gleichung, also auch die Entwickelung von $K = \frac{\sqrt{1}+10}{9}$ stimmt mit der im vorhergehenden Paragraphen überein. Die rechte Seite k aber ist $= 0$ genommen. In diesem Falle stellt schon die Entwickelung von K zwei Auflösungen, nämlich

$$x = M_0 = 1 \text{ und } M_2 = 11$$
$$y = N_0 = 1 \quad\quad N_2 = 9$$

heraus. Wir wollen jedoch zeigen, dass man alle in der Entwickelung von K unmittelbar vorkommenden Auflösungen un-

beachtet lassen kann, indem sich dieselben durch die Kombinationen zwischen K und K' nothwendig ergeben müssen.

Man hat hier für die beiden durch $k=0$ theilbaren Zahlen von der Form $1-p^2$ die Werthe $p=\pm 1$. Der erste Werth gibt $K'=\frac{\sqrt{1}+1}{0}$. Q'_{-1} ist hier willkürlich, und kann nach §. 91 $=0$ oder $=1$ gesetzt werden. Soll der Schluss mit dem von K übereinstimmen; so ist $Q'_{-1}=1$ zu nehmen. Dies gibt

n	P'_n	Q'_n	a'_n
-1		1	
0	1	0	

Kombinirt man nun hier, wo wegen $k=0$ die Zeigersumme $m+m'$ sowol paar wie unpaar sein darf, $K(3)$ *komb.* $K'(0)=K(3)$; so ergibt Dies nach der Entwickelung von K die Auflösung $x=11$, $y=9$.

Der zweite Werth von K' ist $\frac{\sqrt{1}-1}{0}$. Hierin ist Q'_{-1} ebenfalls willkürlich $=0$ oder $=1$. Der Werth $Q'_{-1}=0$ muss verworfen werden. Der Werth $Q'_{-1}=1$ dagegen liefert unter Berücksichtigung des §. 90 folgende Entwickelung mit einem Schlusse in kleinsten positiven Zahlen.

n	P'_n	Q'_n	a'_n
-1		1	
0	-1	0	0
1	1	1	2
2	1	0	

Da dieser Schluss mit dem von K übereinstimmt; so ergibt die Kombination $K(2)$ *komb.* $K'(1)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	4	5	4
2	0	1	1

die Auflösung $x=1$, $y=1$.

Die allgemeinen Auflösungen der gegebenen Gleichung sind also

$$x=11w=\ldots-33,\ -22,\ -11,\ 0,\ 11,\ 22,\ 33\ldots$$
$$y=9w=\ldots-27,\ -18,\ -9,\ 0,\ 9,\ 18,\ 27\ldots$$

und

$$x=w=\ldots,-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3\ldots$$
$$y=w=\ldots,-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3\ldots$$

§. 111. *Beispiel mit quadratischer Determinante:*

$$x^2-y^2=24.$$

Hier ist $a=1$, $b=0$, $c=1$, also $D=b^2+ac=0^2+1.1=1$ und $K=\frac{\sqrt{1}+0}{1}$. Dies gibt

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		1		1	0
0	0	1	1	1	1
1	1	0			

Es gibt hier 8 Reihen der durch $k = 24$ theilbaren Zahlen von der Form $1 - p^2$, für welche $p = \pm 1, \pm 5, \pm 7, \pm 11$ ist. Man findet jedoch, dass nur die beiden Werthe $p = -5$ und $p = -11$ brauchbare Werthe für K' ergeben.

Der erste Werth gibt $K' = \frac{\sqrt{1} - 5}{24}$ und

n	P'_n	Q'_n	a'_n
-1		-1	
0	-5	24	-1
1	-19	-15	1
2	4	1	5
3	1	0	

Dieser Schluss von K' stimmt mit dem von K überein, und es ist $m + m' = 1 + 3 = 4$ eine paare Zahl. Demnach hat man für $K(1)$ *komb.* $K'(3)$

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	0	1	0
2	-5	-4	1
3	-1	5	-1

also $x = 5,\ y = -1$.

Der zweite Werth $K' = \frac{\sqrt{1} - 11}{24}$ gibt

n	P'_n	Q'_n	a'_n
-1		-5	
0	-11	24	-1
1	-13	-7	1
2	6	5	1
3	-1	0	2
4	1	1	2
5	1	0	

Auch dieser Schluss stimmt mit dem von K überein und es ist $m + m' = 1 + 5 = 6$ eine paare Zahl. Demnach hat man

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	0	1	0
2	-2	-1	1
3	-2	3	-2
4	-1	-4	3
5	-1	7	-5

also $x = 7,\ y = -5$.

In diesen beiden Auflösungen können, da $P_0 = 0$ ist, noch die Zeichen von x und y sowol zusammen, als auch einzeln umgekehrt werden.

Da $k = 24 = 2^2 . 6$ den quadratischen Faktor 2^2 besitzt; so sind noch die etwaigen Auflösungen mit dem gemeinschaftlichen Maasse 2 zu untersuchen. Hierfür kommen die beiden Werthe $p = \pm 1$ in Betracht. Man findet jedoch, dass Dies keine brauchbaren Entwickelungen von K' liefert, dass also keine Auflösungen mit einem gemeinschaftlichen Maasse vorhanden sind.

§. 112. ***Beispiel mit quadratischer Determinante:***

$$3x^2 - 14xy = 5.$$

Hier ist $a = 3$, $b = 7$, $c = 0$, also $D = b^2 + ac = 7^2 + 3 . 0 = 49$ und $K = \frac{\sqrt{49} + 7}{3}$. Dies gibt folgende Entwickelung mit einem Schlusse in kleinsten positiven Zahlen:

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		0		1	0
0	7	3	4	4	1
1	5	8	1	5	1
2	3	5	2	14	3
3	7	0			

Es gibt zwei Reihen der durch $k = 5$ theilbaren Zahlen J von der Form $49 - p^2$, für welche $p = \pm 2$ ist. Der erste Werth $K' = \frac{\sqrt{49} + 2}{5}$ liefert die Entwickelung

n	P'_n	Q'_n	a'_n
-1		9	
0	2	5	1
1	3	8	1
2	5	3	4
3	7	0	

Dieser Schluss in kleinsten positiven Zahlen stimmt nicht mit dem von K überein. Demnach führt dieser Werth von K' zu keiner Auflösung.

Der zweite Werth $K' = \frac{\sqrt{49} - 2}{5}$ entwickelt sich in

n	P'_n	Q'_n	a'_n
-1		9	
0	-2	5	1
1	7	0	

Da sich hier ein Schluss einstellt, welcher mit dem von K übereinstimmt, auch $m + m' = 3 + 1 = 4$ eine paare Zahl ist; so erhält man durch die Kombination K (3) *komb.* K' (1)

n	a_n	M_n	N_n
1		5	1
2		14	3
3	0	5	1

die Auflösung $x=5$, $y=1$. Ausser dieser und der mit entgegengesetzten Zeichen ist also keine Auflösung möglich.

Der Übung wegen wollen wir die gegebene Gleichung nochmals lösen, indem wir die Buchstaben x, y mit einander verwechseln, also

$$-14xy+3y^2=5$$

schreiben. Hierin ist $a=0$, $b=7$, $c=-3$, also $D=b^2+ac$ $=7^2+0(-3)=49$ und $K=\frac{\sqrt{49}+7}{0}$. Die Entwickelung von K würde jetzt durch

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-3		1	0
0	7	0			

dargestellt sein. Da dieselbe keinen Schluss in kleinsten positiven Zahlen besitzt; so hat man, um einen solchen *herzustellen*, nach der Gl. (2) in §. 90

$$-3=2.7.0-3 \quad \text{also } R=3$$

Da $w=0$ ist; so ist die Entwickelung von K in der Weise fortzuführen, dass man resp. a_0, a_1, $a_2=-1, 1, -1$ setzt. Dies gibt im Zusammenhange nach §. 88

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-3		1	0
0	7	0	-1	-1	1
1	-7	-17	1	0	1
2	-10	3	-1	-1	0
3	7	0			

Die Werthe von K' sind die früheren. Man erkennt, dass sich nur der erste, nämlich $K'=\frac{\sqrt{49}+2}{5}$ mit K kombiniren lässt, und zwar hat man für $K(3)$ *komb.* $K'(3)$

n	a_n	M_n	N_n
1		0	1
2		-1	0
3	0	0	1
4	-4	-1	-4
5	-1	1	5

also die Auflösung $x=1$, $y=5$, welche mit der vorhin gefundenen übereinstimmt, wenn man x mit y verwechselt.

§. 113. *Beispiel mit quadratischer Determinante:*

$$xy=24.$$

Da in dieser Gleichung der Koeffizient von xy keine paare Zahl ist; so muss dieselbe zuvor mit 2 multiplizirt, und demnach die Gleichung

$$2xy = 48$$

aufgelös't werden. Hierin ist $a = 0$, $b = -1$, $c = 0$, also $D = b^2 + ac = (-1)^2 + 0.0 = 1$ und $K = \frac{\sqrt{1} - 1}{0}$. Dieser Ausdruck ist nach §. 91 zum Schlusse zu führen, indem man beachtet, dass Q_{-1} den bestimmten Werth 0 hat. Es ist jedoch bequemer, die vorstehende Gleichung mit -1 zu multipliziren, und demnach

$$-2xy = -48$$

zu schreiben. Hierin ist $a = 0$, $b = 1$, $c = 0$, also $D = b^2 + ac = 1^2 + 0.0 = 1$ und $K = \frac{\sqrt{1} + 1}{0}$. In dieser Form ist der Schluss bereits erreicht, indem man hat

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		0		1	0
0	1	0			

Es gibt hier für $k = -48$ im Ganzen 8 Reihen der durch 48 theilbaren Zahlen J von der Form $1 - p^2$, für welche resp. $p = \pm 1, \pm 7, \pm 17, \pm 23$ ist. Man findet jedoch, dass nur die vier Werthe $p = \pm 1$ und $p = \pm 17$ zu einem mit dem von K übereinstimmenden Schlusse führen. Für den ersten Werth hat man $K' = \frac{\sqrt{1} + 1}{-48}$

n	P'_n	Q'_n	a'_n
-1		0	
0	1	-48	-1
1	47	46	1
2	-1	0	23
3	1	0	

Obgleich dieser Schluss von K' mit dem von K übereinstimmt; so führt derselbe doch nach der vorstehenden Entwickelung zu keiner Auflösung, weil die Zeigersumme $m + m' = 0 + 3 = 3$ eine unpaare Zahl ist.

Man weiss aber aus §. 90, dass der Schluss 1, 0, 0, in welchem das vorletzte $Q = 0$ ist, in einem Abstande von 3 Gliedern nochmals reproduzirt werden kann, indem man hier $a_3, a_4, a_5 = -1, 1, -1$ setzt. Dies gibt im Zusammenhange für K' folgende Entwickelung nach §. 88

n	P'_n	Q'_n	a'_n
-1		0	
0	1	-48	-1
1	47	46	1
2	-1	0	23
3	1	0	-1
4	-1	-2	1
5	-1	0	-1
6	1	0	

Bildet man jetzt die Kombination $K(0)$ *komb.* $K'(6)$; so ergibt sich

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	-1	-1	0
3	1	0	1
4	-23	-1	-23
5	-1	1	24

also die Auflösung $x = 1$, $y = 24$.

Für den zweiten Werth $K = \frac{\sqrt{1} - 1}{-48}$ hat man

n	P'_n	Q'_n	a'_n
-1		0	
0	-1	-48	0
1	1	0	

Dies ist kein Schluss in kleinsten positiven Zahlen. Um einen solchen zu erhalten, hat man nach Gl. (2) in §. 90

$$Q'_0 = -48 = 2.1(-24) - 0, \text{ also } R = 0$$

und da $w = -24$ ist, $a'_1 = 23$, $a'_2 = 1$, $a'_3 = -1$. Dies gibt im Zusammenhange nach §. 88

n	P'_n	Q'_n	a'_n
-1		0	
0	-1	-48	0
1	1	0	23
2	-1	-2	1
3	-1	0	-1
4	1	0	

Jetzt kann man bilden $K(0)$ *komb.* $K'(4)$. Dies gibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	-1	-1	0
3	-23	24	1

also die Auflösung $x = 24$, $y = 1$.

Der dritte Werth $K' = \frac{\sqrt{1} + 17}{-48}$ liefert, wenn man die entstehende Entwickelung, welche bei dem Zeiger 5 schliesst, nach Art der Entwickelung von $\frac{\sqrt{1} + 1}{-48}$ noch um drei Glieder fortsetzt,

n	P'_n	Q'_n	a'_n
-1		6	
0	17	-48	-1
1	31	20	1
2	-11	-6	1
3	5	4	1
4	-1	0	2
5	1	0	-1
6	-1	-2	1
7	-1	0	-1
8	1	0	

Kombinirt man jetzt $K(0)$ *komb.* $K'(8)$; so kommt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	1	1	1
2	-1	-1	0
3	1	0	1
4	-2	-1	-2
5	-1	1	3
6	-1	-2	-5
7	-1	3	8

also $x = 3$, $y = 8$.

Der vierte Werth $K' = \frac{\sqrt{1} - 17}{-48}$ gibt

n	P'_n	Q'_n	a'_n
-1		6	
0	-17	-48	0
1	17	6	3
2	1	0	

Dies ist kein Schluss in kleinsten positiven Zahlen. Um einen solchen zu erhalten, hat man nach Gl. (1) in §. 90

$$Q'_1 = 6 = 2 . 1 . 3 + 0, \quad \text{also } R = 0$$

und da $w = 3$ ist, $a'_2 = -3$, $a'_3 = 0$, folglich im Zusammenhange nach §. 88

n	P'_n	Q'_n	a'_n
-1		6	
0	-17	-48	0
1	17	6	3
2	1	0	-3
3	-1	0	0
4	1	0	

Bildet man nun $K(0)$ *komb.* $K'(4)$; so ergibt sich

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	0	1	0
2	3	3	1
3	-3	-8	-3

also $x = -8$, $y = -3$.

Die vorstehenden vier Auflösungen können noch mit entgegengesetzten Zeichen genommen werden. Ausser ihnen gibt es keine in relativ primen Zahlen.

Um die Auflösungen mit gemeinschaftlichem Maasse zu untersuchen, beachte man, dass $k = -48 = (2 \,.\, 2)^2 (-3)$ ist. Man hat also zuerst nachzusehen, ob es Auflösungen mit dem gemeinschaftlichen Maasse 2, und dann, ob es solche mit dem gemeinschaftlichen Maasse $2 \,.\, 2 = 4$ gibt.

Für die erste Untersuchung hat man $k = \alpha^2 k' = 2^2 (-12)$ also $k' = -12$. Die durch 12 theilbaren Zahlen von der Form $1 - p^2$ entsprechen den vier Werthen $p = \pm 1, \pm 5$, woraus sich die vier Werthe $K' = \frac{\sqrt{1} \pm 1}{-12}, \frac{\sqrt{1} \pm 5}{-12}$ ergeben. Die Entwickelung eines jeden dieser vier Werthe kann zu einem mit K übereinstimmenden Schlusse gebracht werden, und Dies führt zu den Werthen

$$x' = 1,\ 6,\ 2,\ 3, \text{ also } x = 2,\ 12,\ 4,\ 6,$$
$$y' = 6,\ 1,\ 3,\ 2, \qquad y = 12,\ 2,\ 6,\ 4,$$

welche ebenfalls mit entgegengesetzten Zeichen genommen werden können.

Für die zweite Untersuchung hinsichtlich der Auflösungen mit dem gemeinschaftlichen Maasse 4 ist $k = \alpha^2 k' = 4^2 (-3)$ also $k' = -3$ zu nehmen. Die durch 3 theilbaren Zahlen von der Form $1 - p^2$ entsprechen den beiden Werthen $p = \pm 1$ also auch den beiden Werthen $K' = \frac{\sqrt{1} \pm 1}{-3}$. Es kann jedoch der Schluss keines dieser Werthe von K' mit dem von K in Übereinstimmung gebracht werden, weshalb es keine Auflösungen mit dem gemeinschaftlichen Maasse 4 gibt.

§. 114. *Beispiel mit der Determinante null.*

Wenn die Gleichung

$$ax^2 - 2bxy - cy^2 = k$$

nicht von vorn herein unmöglich sein soll; so dürfen, nachdem die vier Koeffizienten a, $2b$, c, k von ihrem etwaigen gemeinschaftlichen Maasse befreiet sind, die drei Koeffizienten a, $2b$, c kein gemeinschaftliches Maass mehr enthalten. Soll nun bei dieser Voraussetzung die Determinante $D = b^2 + ac = 0$, also $-ac = b^2$ sein; so müssen die beiden Koeffizienten a und c entgegengesetzte Zeichen haben, und ausserdem muss der absolute Werth sowol von a wie von c ein vollständiges Quadrat sein. Denn wäre Dies nicht der Fall; so müsste, damit das Produkt $-ac$ ein Quadrat b^2 sein kann, a und c einen gemeinschaftlichen Faktor enthalten, welcher dann auch wegen $-ac = b^2$ ein Faktor von b wäre, sodass nun a, b, c und mithin auch

a, $2b$, c ein gemeinschaftliches Maass besässen, was der Voraussetzung widerspricht. Wäre a negativ; so kann man durch Multiplikation der gegebenen Gleichung mit -1 dafür sorgen, dass a positiv wird. Alsdann muss c negativ werden.

Wenn aber $a = f^2$, $c = -g^2$ und $-ac = b^2 = f^2 g^2$ also $b = fg$ ist; so ist die linke Seite der gegebenen Gleichung

$$ax^2 - 2bxy - cy^2 = f^2 x^2 - 2fgxy + g^2 y^2 = (fx - gy)^2$$

also ein vollständiges Quadrat, worin jedoch f und g sowol positiv wie negativ sein können, so jedoch, dass $fg = b$ ist, also das Produkt fg das Zeichen von b hat.

Hieraus folgt, dass auch die rechte Seite k ein vollständiges Quadrat, mithin entschieden positiv sein muss. Die gegebene quadratische Gleichung zerfällt also, wenn die Determinante $D = 0$ ist, durch Wurzelausziehung auf beiden Seiten stets in zwei Gleichungen vom ersten Grade, welche durch

$$fx - gy = \pm \sqrt{k}$$

dargestellt sind.

Wir werden jedoch die gegebene quadratische Gleichung genau nach dem in §. 100 erläuterten Prinzipe behandeln, und als Beispiel die Gleichung

$$4x^2 + 12xy + 9y^2 = 9$$

auflösen, welche in die beiden Gleichungen $2x + 3y = \pm 3$ vom ersten Grade zerfallen würde.

Hier ist $a = 4$, $b = -6$, $c = -9$, also $D = b^2 + ac$ $= (-6)^2 + 4(-9) = 0$ und $K = \frac{\sqrt{0} - 6}{4}$. Die Entwickelung hiervon nach §. 93 ist

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-9		1	0
0	-6	4	-2	-2	1
1	-2	-1	2	-3	2
2	0	0			

Dies ist kein Schluss in positiven Zahlen. Um einen solchen zu erzeugen, und um zugleich eine willkürliche Zahl w in die Quotientenreihe einzuführen, setzen wir diese Entwickelung nach §. 93 noch um die Quotienten $a_2 = w$, $a_3 = 1$, $a_4 = -1$ fort. Dies gibt im Zusammenhange

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-9		1	0
0	-6	4	-2	-2	1
1	-2	-1	2	-3	2
2	0	0	w	$-2-3w$	$1+2w$
3	0	-1	1	$-5-3w$	$3+2w$
4	-1	1	-1	3	-2
5	0	0			

Jetzt sind die Reihen der durch $k=9$ theilbaren Zahlen J von der Form $0-p^2$ zu suchen. Es gibt deren drei für $p=0, \pm 3$. Der erste Werth $K'=\frac{\sqrt{0}+0}{9}$, welcher die Entwickelung

n	P'_n	Q'_n	a'_n
-1		0	
0	0	9	0
1	0	0	

liefert, besitzt einen mit K nicht übereinstimmenden Schluss.

Der zweite Werth $K'=\frac{\sqrt{0}+3}{9}$ liefert

n	P'_n	Q'_n	a'_n
-1		-1	
0	3	9	0
1	-3	-1	3
2	0	0	

Dieser Schluss von K' stimmt, wenn er nach §. 93 in einen Schluss mit positiven Zahlen verwandelt wird, mit dem von K überein. Es wird für den neuen Schluss auch die Zeigersumme $m+m'=5+5=10$ eine paare Zahl sein, also eine Auflösung liefern. Bei der Bildung dieses Schlusses von K' nach §. 93 ist es übrigens nicht nöthig, noch fernerweit eine Willkürliche in die Quotientenreihe einzuführen. Man kann vielmehr einfach $a'_2=0$, $a'_3=1$, $a'_4=-1$ nehmen. Dies gibt im Zusammenhange

n	P'_n	Q'_n	a'_n
-1		-1	
0	3	9	0
1	-3	-1	3
2	0	0	0
3	0	-1	1
4	-1	1	-1
5	0	0	

Bildet man nun $K(5)$ *komb.* $K'(5)$; so kommt

n	a_n	M_n	N_n
3		$-5-3w$	$3+2w$
4		3	-2
5	0	$-5-3w$	$3+2w$
6	1	$-2-3w$	$1+2w$
7	-1	-3	2
8	0	$-2-3w$	$1+2w$
9	-3	$3+9w$	$-1-6w$

also die Auflösung $x=3+9w$, $y=-1-6w$, worin w irgend eine ganze Zahl darstellt.

Der dritte Werth $K'=\frac{\sqrt{0}-3}{9}$ gibt

n	P'_n	Q'_n	a'_n
-1		-1	
0	-3	9	-1
1	-6	-4	1
2	2	1	2
3	0	0	

Dieser Schluss stimmt mit dem von K überein, und es ist auch die Zeigersumme $m+m'=5+3=8$ eine paare Zahl. Kombinirt man demnach $K(5)$ *komb.* $K'(3)$; so erhält man

n	a_n	M_n	N_n
3		$-5-3w$	$3+2w$
4		3	-2
5	0	$-5-3w$	$3+2w$
6	-2	$13+6w$	$-8-4w$
7	-1	$-18-9w$	$11+6w$

also $x=-18-9w$, $y=11+6w$.

Jede der vorstehenden beiden Auflösungen kann auch mit entgegengesetztem Zeichen genommen werden, was bei der Willkürlichkeit der Grösse w auf eine Umkehrung des Zeichens der in den Ausdrücken von x und y vorkommenden Konstanten hinausläuft. Die bis jetzt gefundenen Auflösungen werden immer, welchen Werth man auch für w setzen möge, relativ prim sein.

Bei allen Gleichungen mit der Determinante $D=0$ wird die rechte Seite k, da sie selbst ein Quadrat ist, quadratische Faktoren enthalten, deren Absonderung, wennicht gerade $k=1$ ist, zu neuen Auflösungen mit einem gemeinschaftlichen Maasse führt. Hier, wo $k=9=3^2.1$ ist, kann man den quadratischen Faktor $\alpha^2=3^2$ absondern, was Auflösungen mit dem gemeinschaftlichen Maasse $\alpha=3$ ergeben wird.

Die durch $k'=1$ theilbaren Zahlen von der Form $0-p^2$ bilden eine einzige Reihe, für welche $p=0$, also $K'=\frac{\sqrt{0}+0}{1}$ ist.

Dieser Werth von K' liefert die Entwickelung

n	P'_n	Q'_n	a'_n
-1		0	
0	0	1	0
1	0	0	

Bildet man $K(5)$ *komb.* $K'(1)$; so kommt

n	a_n	M_n	N_n
3		$-5-3w$	$3+2w$
4		3	-2
5	0	$-5-3w$	$3+2w$

also $x'=-5-3w$, $y'=3+2w$, folglich als Auflösung der gegebenen Gleichung mit dem gemeinschaftlichen Maasse 3 $x=-15-9w$, $y=9+6w$. Auch diese Auflösung kann mit entgegengesetztem Zeichen genommen werden.

Wir bemerken noch, dass es den Anschein hat, als ob die obige Entwickelung von K zwei Auflösungen der Gleichung $4x'^2 + 12x'y' + 9y'^2 = 1$ erkennen liesse, indem sowol $(-1)^3 Q_3 =$, wie auch $(-1)^4 Q_4$ gleich 1 ist. Allein die betreffenden beiden Auflösungen $x' = -2 - 3w$, $y' = 1 + 2w$ und $x' = -5 - 3w$, $y' = 3 + 2w$ sind wegen der Willkürlichkeit von w identisch.

Es wird stets leicht sein, zu erkennen, welche der durch vorstehende Methode gefundenen Auflösungen der Gleichung $f^2x^2 - 2fgxy + g^2y^2 = k$ die Gleichung $fx - gy = +\sqrt{k}$ und welche die Gleichung $fx - gy = -\sqrt{k}$ erfüllen. Demnach wird man umgekehrt im Stande sein, die Gleichung $fx - gy = \pm\sqrt{k}$ vom ersten Grade durch die obige Methode zu lösen, indem man dieselbe quadrirt und die Gleichung $f^2x^2 - 2fgxy + g^2y^2 = k$ behandelt; nach geschehener Auflösung aber nur diejenigen Auflösungen beibehält, welche dem gegebenen Zeichen von $\pm\sqrt{k}$ entsprechen.

Ein solches Verfahren behuf Auflösung einer *unbestimmten* Gleichung vom ersten Grade ist zwar nicht einfacher, als das im dritten Abschnitte gelehrte. Es ist aber insofern beachtenswerth, weil man dadurch ein Mittel erhält, die allgemeinen Formeln derjenigen Auflösungen gesondert darzustellen, welche relativ prim sind und welche ein gemeinschaftliches Maass besitzen, wobei sogar die Sonderung nach der Verschiedenheit des gemeinschaftlichen Maasses selbst eintritt.

So würde z. B. die Auflösung der Gleichung $2x + 3y = 3$ nach dem dritten Abschnitte durch die allgemeine Formel

$$x = 3w = \ldots -12,\ -9,\ -6,\ -3,\ 0,\ 3,\ 6,\ 9,\ 12 \ldots$$
$$y = 1 - 2w = \ldots\ 9,\ 7,\ 5,\ 3,\ 1,\ -1,\ -3,\ -5,\ -7 \ldots$$

dargestellt sein, worin relativ prime und nicht relativ prime Auflösungen untermischt enthalten sind.

Die Auflösungen der quadrirten Gleichung $(2x + 3y)^2 = 4x^2 + 12xy + 9y^2 = 9$, welche zugleich die gegebene Gleichung vom ersten Grade erfüllen, sind dagegen nach Obigem für die relativ primen Werthe

$$x = 3 + 9w = \ldots -15,\ -6,\ 3,\ 12,\ 21 \ldots$$
$$y = -1 - 6w = \ldots\ 11,\ 5,\ -1,\ -7,\ -13 \ldots$$

und

$$x = 18 + 9w = \ldots -9,\ 0,\ 9,\ 18,\ 27 \ldots$$
$$y = -11 - 6w = \ldots\ 7,\ 1,\ -5,\ -11,\ -17 \ldots$$

und ferner für die Werthe mit dem gemeinschaftlichen Maasse 3

$$x = 15 + 9w = \ldots -12,\ -3,\ 6,\ 15 \ldots$$
$$y = -9 - 6w = \ldots\ 9,\ 3,\ -3,\ -12 \ldots$$

§. 115. **Beispiel mit negativer Determinante:**

$$3x^2 - 10xy + 11y^2 = 27.$$

Wenn die Determinante $D = b^2 + ac$ negativ werden soll; so müssen a und c nothwendig entgegengesetzte, also a und $-c$ gleiche Zahlen besitzen und aus §. 95 folgt, dass weil jeder denkbare Werth von $(-1)^n Q_n$ das Zeichen von $Q_0 = a$ hat, die rechte Seite k der gegebenen Gleichung nur positiv oder negativ sein kann, jenachdem a es ist.

Im vorstehenden Beispiele ist $a = 3$, $b = 5$, $c = -11$, also $D = b^2 + ac = 5^2 + 3(-11) = -8$ und $K = \frac{\sqrt{-8} + 5}{3}$. Um sofort in der Entwickelung von K die Periode in kleinsten Zahlen zu treffen, entwickeln wir nach §. 96 erst den absoluten Werth von $\frac{P_0}{Q_0} = \frac{b}{a} = \frac{5}{3}$ in einen Kettenbruch; Dies gibt $\frac{5}{3} = [1, 1, 2]$; und nehmen nun hier, wo $\frac{P_0}{Q_0}$ positiv ist, die wahren Werthe der gefundenen Quotienten als Quotienten einer Entwickelung von K an. Dies gibt

n	P_n	Q_n	a_n
-1		-11	
0	5	3	1
1	-2	-4	1
2	-2	3	2
3	8	-24	

Das Minimum von Q ist also 3. Dasselbe kommt in dieser Entwickelung zweimal resp. als Q_0 und als Q_2 vor. Um also die Periode in kleinsten Zahlen zu erhalten, hat man die vorstehende Entwickelung Ein Mal vom Quotienten a_0 und ein anderes Mal vom Quotienten a_2 an nach der Regel des §. 94 mit grössten reellen Subquotienten fortzusetzen. Bei der ersteren Entwickelung stellt sich der zweite periodische Werth von $Q = -4$, bei der letzteren Entwickelung dagegen $= -3$ heraus. Die letztere führt also zu der gesuchten Periode in kleinsten Zahlen und man hat im Zusammenhange

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-11		1	0
0	5	3	1	1	1
1	-2	-4	1	2	1
2	-2	3	-1	-1	0
3	-1	-3	0	2	1
4	1	3	0	-1	0

Jetzt sind die Reihen der durch $k = 27$ theilbaren Zahlen J von der Form $-8 - p^2$ zu suchen. Es gibt deren zwei für $p = \pm 10$. Zuerst hat man also $K' = \frac{\sqrt{-8} + 10}{27}$. Da die vor-

stehende Entwickelung von K alle Minima von Q erkennen lässt; so kann es eine Ersparung von Rechenarbeit nach sich ziehen, wenn man nicht gleich darauf ausgeht, die Werthe von K' sofort mit einer Periode in kleinsten Zahlen zu entwickeln, vielmehr vorläufig erst einmal nach §. 94 verfährt, um zu sehen, ob nicht die hierdurch sich ergebende Entwickelung mit der von K kombinirt werden kann.

Demnach liefert $K' = \frac{\sqrt{-8}+10}{27}$

n	P'_n	Q'_n	a'_n
-1		-4	
0	10	27	0
1	-10	-4	2
2	2	3	0
3	-2	-4	0

Man sieht, dass sofort die Kombination K (1) *komb.* K' (3), für welche auch die Zeigersumme $m + m' = 1 + 3 = 4$ eine paare Zahl ist, gebildet werden kann. Demnach hat man

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	0	1	0
2	0	1	1
3	-2	-1	-2

folglich $x = -1$, $y = -2$.

Der zweite Werth $K' = \frac{\sqrt{-8}-10}{27}$ stellt bei der gewöhnlichen Entwickelung nach §. 94 kein Glied heraus, welches mit einem Gliede von K übereinstimmte. Demnach wollen wir sofort den Schluss in kleinsten Zahlen von K' aufsuchen. Der absolute Werth von $\frac{p}{k} = \frac{-10}{27}$ ist $\frac{10}{27} = [0, 2, 1, 2, 3]$. Da $\frac{p}{k}$ negativ ist; so hat man die Zeichen dieser Quotienten umzukehren, also 0, -2, -1, -2, -3 als die ersten Quotienten der Entwickelung von $K' = \frac{\sqrt{-8}-10}{27}$ anzunehmen. Dies gibt

n	P'_n	Q'_n	a'_n
-1		-4	
0	-10	27	0
1	10	-4	-2
2	-2	3	-1
3	1	-3	-2
4	5	11	-3
5	-38	-132	

Da diese Entwickelung von K' bei dem Zeiger 2 mit der von K bei dem Zeiger 2 übereinstimmt; so kann man die Kombination K (2) *komb.* K' (2) sofort ausführen, ohne erst die

Periode in kleinsten Zahlen von K' herzustellen, welche nothwendig mit der von K übereinstimmen muss. Dies gibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	0	1	1
3	2	4	3

also $x = 4$, $y = 3$.

Ausser den vorstehenden beiden Auflösungen, welche auch noch mit entgegengesetzten Zeichen genommen werden können, gibt es keine in relativ primen Zahlen. Da aber die rechte Seite der gegebenen Gleichung $k = 27 = 3^2 . 3$ ist; so sind noch die Auflösungen mit dem gemeinschaftlichen Maasse 3 zu untersuchen, indem man jetzt $\alpha^2 k' = 3^2 . 3$ also $\alpha = 3$, $k' = 3$ hat.

Die durch 3 theilbaren Zahlen J von der Form $-8-p^2$ entsprechen den beiden Werthen $p = \pm 1$. Dies bedingt die beiden Werthe $K' = \frac{\sqrt{-8} \pm 1}{27}$. Solche zwei Werthe von K' können höchstens zwei dem absoluten Werthe nach verschiedene Auflösungen der Gleichung $3x'^2 - 10x'y' + 11y'^2 = 3$ nach sich ziehen. Da wir nun erkennen, dass in der obigen Entwickelung von K unter den Grössen $(-1)^n Q_n$ der Werth 3 mehrmals vorkommt, dass aber die entsprechenden Werthe von M und N nur zwei numerisch verschiedenen Auflösungen, nämlich $x' = 1$, $y' = 0$ und $x' = 2$, $y' = 1$ angehören; so ist klar, dass die letzteren die beiden gesuchten Auflösungen für x', y' sind. Demnach hat man, ohne K' weiter zu entwickeln, sofort noch folgende zwei Auflösungen für x und y mit dem gemeinschaftlichen Maasse 3

$$x = 3x' = 3, \quad 6$$
$$y = 3y' = 0, \quad 3$$

welche ebenfalls noch mit entgegengesetzten Zeichen genommen werden können.

§. 116. *Beispiel mit negativer Determinante:*

$$5x^2 + 3y^2 = 3$$

Hier ist $a = 5$, $b = 0$, $c = -3$, also $D = b^2 + ac = 0^2 + 5(-3) = -15$ und $K = \frac{\sqrt{-15} + 0}{5}$. Wenn, wie hier $P_0 = b = 0$ also auch $\frac{P_0}{Q_0} = 0$ ist, so führt nach §. 96 die gewöhnliche Entwickelung von K sogleich zu der Periode in kleinsten Zahlen. Man hat also für K

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-3		1	0
(0	0	5	0	0	1
(1	0	-3	0	1	0

Es gibt Eine symmetrische Reihe der durch $k = 3$ theilbaren Zahlen J von der Form $-15 - p^2$. Man hat dafür $p = 0$, also $K' = \frac{\sqrt{-15} + 0}{3}$. Die für K' sich ergebende Periode wird nicht mit der von K übereinstimmen; sie wird sich aber nur durch das Zeichen der Grössen Q von jener unterscheiden. Da nun die Grössen P in dieser Periode $= 0$ sind; so kann man nach §. 96 durch Anfügung der Quotienten 1, -1, 1 eine mit der von K genau übereinstimmende Periode erzeugen. Dies gibt für K'

n	P'_n	Q_n	a'_n
-1		-5	
0	0	3	1
1	3	-8	-1
2	5	5	1
3	0	-3	0.
4	0	5	0

Durch Kombination von K (1) *komb.* K' (3) erhält man

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	0	1	0
2	-1	-1	1
3	1	0	1

also die einzige Auflösung $x = 0$, $y = 1$, in welcher wegen $P_0 = 0$ der Werth von x und der von y für sich mit entgegengesetztem Zeichen genommen werden kann.

Nachdem man eingesehen hatte, dass es nur Einen Werth von K', also auch nur Eine Auflösung gab, konnte man dieselbe, ohne die Entwickelung von K' zu Hülfe zu nehmen, sofort aus der Entwickelung von K entnehmen, worin der Werth 3 unter den Grössen $(-1)^n Q_n$ vorkommt.

§. 117. **Beispiel mit negativer Determinante:**

$$x^2 + y^2 = 25.$$

I. In dieser Gleichung, worin $a = 1$, $b = 0$, $c = -1$, also $D = b^2 + ac = 0^2 + 1(-1) = -1$ und $K = \frac{\sqrt{-1} + 0}{1}$ ist, besteht die Aufgabe, e i n e g e g e b e n e Z a h l i n z w e i Q u a d r a t e z u t h e i l e n. Die Entwickelung von K ist

n	P_n	Q_n	a_n	M_n	N_n
-2				0	1
-1		-1		1	0
(0	0	1	0	0	1
(1	0	-1	0	1	0

Es gibt zwei Reihen der durch $k=25$ theilbaren Zahlen J von der Form $-1-p^2$, für welche $p=\pm 7$ ist. Schon die gewöhnliche Entwickelung des ersten Werthes von K', welcher $\frac{\sqrt{-1}+7}{25}$ ist, muss immer, wenn die Determinante D den numerischen Werth 1 hat, zu einer Periode in kleinsten Zahlen führen. Man hat

n	P'_n	Q'_n	a'_n
-1		-2	
0	7	25	0
1	-7	-2	3
2	1	1	1
3	0	-1	0
(4	0	1	0
(5	0	-1	0

Diese Periode stimmt mit der von K überein, auch so, dass die Zeigersumme $m+m'$ eine paare Zahl ist. Bildet man demnach $K(0)$ *komb.* $K'(4)$; so kommt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	0	1	0
2	-1	-1	1
3	-3	4	-3

also $x=4$, $y=-3$. Der zweite Werth $K'=\frac{\sqrt{-1}-7}{25}$ liefert

n	P'_n	Q'_n	a'_n
-1		-2	
0	-7	25	-1
1	-18	-13	1
2	5	2	2
3	-1	-1	1
(4	0	1	0
(5	0	-1	0

Diese Periode stimmt ebenfalls mit der von K überein, und die Kombination $K(0)$ *komb.* $K'(4)$ gibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	-1	1	-1
2	-2	-2	3
3	-1	3	-4

also $x=3$, $y=-4$.

In den vorstehenden Auflösungen können wegen $P_0 = 0$ die Zeichen von x und y sowol einzeln, wie zusammen umgekehrt werden.

II. Wir müssen darauf aufmerksam machen, dass wenn in einer Periode $P = 0$ ist, wie im gegenwärtigen Falle, man nach §. 96 durch die Quotienten 1, —1, 1 eine andere Periode erzeugen kann, in welcher ebenfalls $P = 0$ ist, während die Grössen Q die entgegengesetzten Zeichen haben. Sind nun aber, wie hier, die numerischen Werthe der beiden periodischen Grössen Q einander gleich; so wird die neue Periode mit der früheren ganz identisch sein, und zwar erzeugt sich immer dieselbe Periode, gleichviel, ob man a_n, a_{n+1}, a_{n+2}, oder ob man Einen Zeiger tiefer a_{n+1}, a_{n+2}, a_{n+3} resp. $= 1, -1, 1$ annimmt. Trotz dieser Übereinstimmung der neuen Periode mit der alten, *ist* die Bildung derselben wichtig, und zwar stellt sich dabei Folgendes heraus.

Ist n der erste Zeiger in der ursprünglichen Periode und nimmt man a_n, a_{n+1}, $a_{n+2} = 1, -1, 1$; so ergebe die Kombination von K und $K' = \frac{\sqrt{-D}+p}{k}$ nach der neuen Periode die Auflösung (A).

Nimmt man dagegen a_{n+1}, a_{n+2}, $a_{n+3} = 1, -1, 1$; so ergebe die Kombination von K und $K' = \frac{\sqrt{-D}+p}{k}$ die Auflösung (B). Andere, als diese beiden Auflösungen (nach ihrem numerischen Werthe) können aus keiner Kombination von K und K' hervorgehen, welche beliebige Entwickelung man auch mit K vornehmen möge.

Kombinirt man nun mit K den zweiten Werth von K', in welchem p das entgegengesetzte Zeichen hat, also den Werth $K' = \frac{\sqrt{-D}-p}{k}$; so ergeben sich in ähnlicher Weise zwei Auflösungen, von denen jedoch die Eine mit (A) und die andere mit (B) übereinstimmt.

Demnach führen also die zwei Werthe $K' = \frac{\sqrt{-D}\pm p}{k}$ immer nur zu zwei verschiedenen Auflösungen, und man wird in den meisten Fällen nicht nöthig haben, K in der oben angegebenen Weise mit den beiden Perioden zu entwickeln; vielmehr wird man sich darauf beschränken können, die gewöhnliche Entwickelung von K Ein Mal mit $K' = \frac{\sqrt{-D}+p}{k}$ und ein anderes Mal mit $K' = \frac{\sqrt{-D}-p}{k}$ zu kombiniren.

Nur in dem Falle, wo $p = 0$ wäre, also die beiden Werthe von K' identisch wären, folglich bei gewöhnlicher Entwickelung sich durchaus übereinstimmend zeigten, müsste die zweifache Periode entweder von K oder von K' in Betracht gezogen werden, um die betreffenden zwei verschiedenen Auflösungen zu erhalten. Dieser Fall tritt ein, sobald man im obigen Beispiele die Auflösungen mit gemeinschaftlichem Maasse aufsucht.

Man hat nämlich $k = 25 = 5^2 . 1 = \alpha^2 k'$. Es ist also nachzusehen, ob es Auflösungen mit dem gemeinschaftlichen Maasse $\alpha = 5$ gibt. Zu dem Ende findet man, dass es nur Eine, und zwar symmetrische Reihe der durch $k' = 1$ theilbaren Zahlen J von der Form $-1 - p^2$ gibt, für welche $p = 0$, also $K' = \frac{\sqrt{-1} + 0}{1}$ ist. Hier sind die beiden Werthe $K' = \frac{\sqrt{-1} \pm 0}{1}$ identisch, und man muss, da sich in der Periode von K und K' die Grösse $P = 0$ und für Q die numerisch gleichen Werthe -1, 1 herausstellen, entweder K oder K' mit den beiden vorhin genannten gleichen Perioden entwickeln und darauf kombiniren.

Die ursprüngliche Entwickelung von K enthält jedoch schon unter den Grössen $(-1)^n Q_n$ den Werth $k' = 1$ mehrere Mal, und man sieht sofort, dass diesem Werthe die beiden verschiedenen Auflösungen $x' = 0$, $y' = 1$ und $x' = 1$, $y' = 0$ entsprechen. Demnach kann man sich alle weitere Rechnung ersparen. Man hat als Auflösungen mit dem gemeinschaftlichen Maasse 5

$$x = 5x' = 0,\ 5$$
$$y = 5y' = 5,\ 0$$

Auch in diesen beiden Auflösungen können noch die Zeichen von x und y einzeln und zusammen umgekehrt werden.

§. 118. *Minima der quadratischen Formen.*

I. Der von zwei Unbekannten x, y abhängige homogene Ausdruck $ax^2 + 2bxy - cy^2$, in welchem jedes Glied vom zweiten Grade ist und das mit beiden Unbekannten behaftete mittlere Glied einen paaren Koeffizienten besitzt, heisst nach Gauss eine binäre quadratische Form, wogegen ähnliche Ausdrücke mit drei, vier etc. Unbekannten ternäre, quaternäre etc. Formen heissen. Wenn man es bei einer Untersuchung immer nur mit quadratischen Formen zu thun hat, welche dieselbe Anzahl von Unbekannten enthalten; so gebraucht man auch der Kürze wegen die allgemeine Bezeichnung quadratische Formen für die eben vorliegende spezielle Gattung.

Die linken Seiten der bisher behandelten unbestimmten Gleichungen vom zweiten Grade sind also quadratische Formen (und zwar binäre). Bei der Auflösung solcher Gleichun-

gen sind alle Kriterien von Wichtigkeit, an welchen man, ohne das ganze Auflösungsverfahren ausführen zu müssen, die Möglichkeit oder Unmöglichkeit der Auflösung erkennen kann. Einige Merkmale dieser Art ergeben sich aus der Untersuchung der Minima, welche eine quadratische Form für alle denkbaren Werthe der Unbekannten x, y anzunehmen vermag. Dabei bemerken wir, dass durch Absonderung der quadratischen Faktoren von dem konstanten Gliede k auf der rechten Seite die Auflösung der Gleichung immer leicht auf eine Auflösung in relativ primen Zahlen zurückgeführt wird. Demnach können wir die Betrachtung auf diejenigen Minima beschränken, welche eine quadratische Form durch die Substitution beliebiger relativ primen Werthe für x und y anzunehmen vermag. Hierdurch ist denn auch die Substitution $x=0$, $y=0$, welche jede willkürliche Zahl zum gemeinschaftlichen Maasse hat und den Werth der quadratischen Form stets auf 0 reduzirt, ausgeschlossen.

Es ist nun wichtig, nicht bloss den kleinsten absoluten Werth, welchen k anzunehmen vermag, sondern auch den *kleinsten* positiven und den kleinsten negativen Werth von k, jeden für sich zu kennen, also resp. das absolute, das positive und das negative Minimum von k zu bestimmen. Ferner ist es wichtig, bis zu einem gewissen Gränzwerthe hinauf, vom Werthe 0 an gerechnet, alle Zahlen zu ermitteln, welche für k auftreten können. Unter dem letzteren Gesichtspunkte kommen dann mehrere unterhalb einer gewissen Gränze liegende Minima von k in Betracht. Bei dieser Untersuchung sind, wie früher, verschiedene Fälle je nach der Beschaffenheit der Determinante $D=b^2+ac$ gesondert zu betrachten.

II. Wenn die Determinante D positiv und kein Quadrat ist; so ist die Kettenbruchsentwickelung von $K=\frac{\sqrt{D}+P_0}{Q_0}=\frac{\sqrt{D}+b}{a}$ unendlich und periodisch. Aus §. 65 und den späteren Untersuchungen erhellet, dass bei keiner Entwickelung von K unter den Grössen Q_n, mithin auch *nicht unter* den Grössen $(-1)^n Q_n=k$ andere Werthe, welche numerisch $<\sqrt{D}$ sind, vorkommen können, als welche in der Periode von K bei grössten Subquotienten zur Erscheinung kommen. Hieraus erkennt man also alle absoluten Minima von k, welche $<\sqrt{D}$ sind. Ist mithin der gegebene Werth von k numerisch $<\sqrt{D}$ und nicht in der Periode der Grössen Q enthalten; so ist die Auflösung (in relativ primen Zahlen) unmöglich. Da der Werth 1 stets $<\sqrt{D}$ sein wird; so ist, wenn $k=\pm 1$ gegeben ist,

die Auflösung jederzeit unmöglich, wenn nicht der Werth $Q=1$ in der fraglichen Periode vorkommt.

In dem Beispiele des §. 103 ist $D=37$. In der Periode der Grössen Q kommen nur die Werthe 3 und 4 vor, welche $<\sqrt{27}$ oder $\leqq 6$ sind. Die rechte Seite jener Gleichung kann also (für relativ prime Werthe von x, y) keinen der absoluten Werthe 0, 1, 2, 5, 6 annehmen.

Da in der Periode der Q stets mindestens Ein Werth $<\sqrt{D}$ vorkommen muss; so folgt, dass es stets möglich ist, den numerischen Werth der quadratischen Form $<\sqrt{D}$ zu machen.

Was die positiven und die negativen Minima von k betrifft, welche numerisch $<\sqrt{D}$ sind; so sind Dies diejenigen Werthe, welche in der Periode der Grössen $(-1)^n Q_n$ vorkommen. Um Dies einzusehen, beachte man, dass wenn der Ausdruck K auf irgend zwei verschiedene Weisen so in einen Kettenbruch entwickelt ist, dass beliebige willkürliche Quotienten vorangehen und von einer gewissen Stelle an nur grösste Subquotienten folgen, die Zeiger der übereinstimmenden Glieder in der Periode der Grössen $(-1)^n Q_n$ aus jenen beiden Entwickelungen stets eine paare Differenz besitzen. Ist nun q irgend ein möglicher Werth von k; so muss derselbe unter den Grössen $(-1)^n Q_n$ in irgend einer Entwickelung von K anzutreffen sein. Denken wir uns, diese Entwickelung sei dargestellt und darin $(-1)^n Q_n = q$, also $Q_n = (-1)^n q = \pm q$. Wäre $(-1)^n q$ positiv; so müsste dasselbe, da es $<\sqrt{D}$ ist, wenn man sich von a_n an lauter grösste Subquotienten genommen denkt, nach §. 65 in der sofort beginnenden Periode der Grössen Q und demnach q in der Periode der Grössen $(-1)^n Q_n$ liegen. Wäre dagegen $Q_n = (-1)^n q$ negativ; so erzeuge man erst nach §. 71 durch Einführung der drei Quotienten $a_n = 1$, $a_{n+1} = -1$, $a_{n+2} = 1$ bei dem Zeiger $n+3$ den entgegengesetzten, also positiven Werth Q_{n+3}. Lässt man jetzt von a_{n+3} an lauter grösste Subquotienten folgen; so muss Q_{n+3} nach §. 65 in der sofort beginnenden Periode der Grössen Q, mithin $(-1)^{n+3} Q_{n+3} = (-1)^n Q_n = q$ in der Periode der Grössen $(-1)^n Q_n$ liegen.

Wenn die Periode von K, also auch die der Grössen Q_n unpaar ist; so enthält bekanntlich die Periode der Grössen $(-1)^n Q_n$, welche stets paar ist, jeden periodischen Werth von Q, also jeden möglichen Werth von k sowol mit positivem, wie auch mit negativem Zeichen.

In dem Beispiele des §. 103, wo die Periode von K dreigliedrig, also die der Grössen $(-1)^n Q_n$ sechsgliedrig ist, hat man also als positive Minima $\leqq 6$ die Werthe 3, 4 und als negative Minima -3, -4. Demnach kann die rechte Seite

jener Gleichung von den Zahlen, welche absolut $\leqq 6$ sind, nur die Werthe ± 3, ± 4 annehmen, wogegen 0, ± 1, ± 2, ± 5, ± 6 unmögliche Werthe von k sind.

Im Beispiele des §. 101, wo $D = 11$, also $\sqrt{D} > 3$ ist, kommen in der zweigliedrigen Periode der Grössen $(-1)^n Q_n$ nur die Werthe -1 und 2 vor. Dieses sind also von allen Zahlen, welche absolut $\leqq 3$ sind, die einzigen, auf die der Werth von k gebracht werden kann. Unmögliche Werthe von k sind in diesem Falle 0, 1, -2, ± 3.

III. Wenn die Determinante D ein Quadrat ist, auch den Fall D gleich null mit eingeschlossen; so kann k stets $= 0$ werden, weil das letzte Q im Schlusse der Entwickelung von K immer $= 0$ ist. Das absolute Minimum der quadratischen Form ist also $= 0$. Wir bemerken noch, dass wenn in einer Entwickelung von K unter den Grössen Q der numerische Werth 1 vorkommt, diese Grösse immer dem vorletzten Werthe des beim nächsten Zeiger erfolgenden Schlusses angehört. Wenn also $k = \pm 1$ ein möglicher Werth sein soll; so muss das vorletzte Q des Schlusses in kleinsten positiven Zahlen (§. 90) den Werth 1 haben, und wenn man dieses Q mit Q_{n-1} bezeichnet, so muss $(-1)^{n-1} Q_{n-1} = k = \pm 1$ sein. (Für $D = 1$ hat man auf die in §. 90 bezeichnete Zweideutigkeit des Schlusses in kleinsten positiven Zahlen zu achten, sobald $Q_{n-1} = 1$ ist, indem alsdann stets $(-1)^{n-1} Q_{n-1} = 1$ und auch $= -1$ gemacht werden kann.)

IV. Wenn die Determinante $-D$ negativ ist; so sind bekanntlich die Werthe der Koeffizienten a und $-c$ entweder beide positiv oder beide negativ. Im ersteren Falle kann k nur positive, im letzteren dagegen nur negative Werthe annehmen. Das Minimum von k ist nach §. 96 zu bestimmen, und macht bekanntlich auch einen Werth von Q in der Periode in kleinsten Zahlen aus. Dasselbe ist stets > 0. Soll also k den absoluten Werth 1 haben; so muss dasselbe offenbar das Minimum von k sein.

Hiernach kann z. B. in dem Beispiele des §. 115 die rechte Seite der gegebenen Gleichung nur positive Werthe > 3 annehmen, da dort das Minimum von $Q = 3$ gefunden ist.

V. Alles Vorstehende setzt voraus, dass für x und y nur relativ prime Zahlen substituirt werden. Bei Zulassung von Zahlen mit gemeinschaftlichem Maasse α ändern sich die Werthe der Minima in leicht zu erkennender Weise.

Zuvörderst aber leuchtet ein, dass wenn x und y das gemeinschaftliche Maass α haben sollen, k den quadratischen Faktor α^2 besitzen muss.

Denkt man sich nun für α nach und nach die Werthe 0, 1, 2, 3... gesetzt; so ist klar, dass für $x = 0$, $y = 0$ jede qua-

dratische Form das Minimum $k=0$ annehmen kann. Schliesst man diesen Werth aus; so leuchtet ferner ein, dass auch für Zahlen mit gemeinschaftlichem Maasse der absolute Werth von k nicht kleiner werden kann, als das kleinste vorhin für die einzelnen Fälle bezeichnete Minimum, indem dieses dem kleinsten gemeinschaftlichen Maasse $\alpha=1$ entspricht. Überhaupt erhält man die Minima von k für irgend ein gegebenes gemeinschaftliches Maass α, indem man die obigen Minima mit α^2 multiplizirt. Auf das Zeichen von k hat das gemeinschaftliche Maass keinen Einfluss.

So würden z. B. in dem Beispiele des §. 103 unter der Bedingung, dass x und y das gemeinschaftliche Maass 3 besässen, da dort $\sqrt{D}>6$ ist, die positiven und negativen Minima, welche $\leqq 3^2.6$ d. i. $\leqq 54$ sind, die numerischen Werthe $3^2.3=27$ und $3^2.4=36$ besitzen.

§. 119. *Reduktion einer quadratischen Gleichung auf eine andere, deren rechte Seite den Werth 1 hat.*

I. Nach vorstehendem Paragraphen zeichnet sich der Fall, wo die rechte Seite der gegebenen Gleichung $k=\pm 1$ ist, dadurch aus, dass wenn dieselbe möglich sein soll, der Werth $(-1)^n Q_n=k=\pm 1$ nothwendig in der Periode, resp. in dem Schlusse in kleinsten Zahlen vorkommen muss.

Bestätigt sich Dies, ist also die Gleichung möglich; so ist auch die Auflösung leicht zu beschaffen; denn für $q=k=\pm 1$ gibt es stets nur eine einzige und zwar symmetrische Reihe der durch q theilbaren Zahlen J von der Form $D-p^2$, für welche $p=0$, also $K'=\frac{\sqrt{D}+0}{\pm 1}$ ist. Man braucht nicht einmal K' in einen Kettenbruch zu entwickeln und mit K zu kombiniren, weil jetzt schon die Entwickelung von K, wenn D ein Quadrat oder negativ ist, die aus einer Kombination mit K' zu erwartende endliche Menge, oder wenn D positiv und nicht quadratisch ist, zwei benachbarte von der aus jener Kombination zu erwartenden unendlichen Menge von Auflösungen ergibt, auf welche man sofort die Rekursionsformel aus §. 84 in Anwendung bringen kann.

Endlich kommen in diesem Falle, wo $k=\pm 1$ keine quadratischen Faktoren >1 besitzt, keine Auflösungen mit gemeinschaftlichem Maasse in Betracht.

Aus allen diesen Gründen ist es interessant, dass man im Stande ist, die Auflösung einer jeden Gleichung, in welcher k einen beliebigen Werth hat, auf die Auflösung einer andern zurückzuführen, in welcher die rechte Seite $=1$ ist.

II. Zu diesem Ende kann man nach Lagranges Zusätzen zu Eulers Algebra, §. 80 in der gegebenen Gleichung

(1) $$ax^2 - 2bxy - cy^2 = k$$

für die Eine Unbekannte x einen Werth von der Form

(2) $$x = py - kz$$

setzen, worin z eine andere Unbekannte ist, und die ganze Zahl p sogleich noch näher bestimmt werden soll.

Was zunächst die Zulässigkeit der Substitution (2) betrifft; so ist klar, dass dieselbe gerechtfertigt sein würde, wenn man überzeugt wäre, dass y und k relativ prim wären, weil alsdann die Gl. (2) wie eine unbestimmte Gleichung vom ersten Grade mit den beiden Unbekannten p und z angesehen werden kann, welche dann nothwendig für p und z ganze Werthe zulassen muss.

Nun erhellet aus Gl. (1), dass wenn y und k ein gemeinschaftliches Maass m besässen, dieses Maass auch in dem Gliede ax^2 enthalten sein müsste. Es kann aber nicht in x^2 enthalten sein, weil x und y als relativ prim vorausgesetzt werden. Demnach müsste m in dem Koeffizienten a enthalten sein.

Hieraus folgt, dass wenn a und k relativ prim sind (also jedenfalls wenn man $a = 1$ hat) auch y mit k relativ prim und folglich die Substitution (2) zulässig ist.

Wenn jedoch a und k irgend ein gemeinschaftliches Maass $m > 1$ besitzen; so reicht die Substitution (2) und die darauf sich stützende weitere Rechnung zur vollständigen Auflösung der Gl. (1) nicht aus; man muss vielmehr noch besonders untersuchen, ob es Werthe von y geben kann, welche ein Vielfaches von m sind. Zu diesem Ende setze man

$$a = ma', \; y = my', \; k = mk'$$

Dies gibt, statt Gl. (1), wenn man dieselbe durch m dividirt, die neue Gleichung

$$a'x^2 - 2bxy' - cmy'^2 = k'$$

welche ebenso, wie die Gl. (1) zu behandeln ist, indem man statt Gl. (2) die folgende setzt

$$x = py' - k'z$$

Für m ist nun nach und nach jedes gemeinschaftliche Maass von a und k zu nehmen und jede daraus sich ergebende Gleichung nach der folgenden Methode für sich zu behandeln.

Durch die Substitution des Werthes von x aus Gl. (2) in Gl. (1) erhält man

$$(ap^2 - 2bp - c)y^2 - 2k(ap - b)yz + ak^2z^2 = k$$

und wenn man durch k dividirt, welche Grösse nicht in y^2 enthalten sein kann, da y und k relativ prim sind, welche also in dem Koeffizienten von y^2 enthalten sein muss,

(3) $\left(\frac{ap^2-2bp-c}{k}\right)y^2-2(ap-b)yz+akz^2=1$

Jetzt bestimmt man die Grösse p so, dass

(4) $$\frac{ap^2-2bp-c}{k}=r \text{ eine ganze Zahl}$$

oder $ap^2-2bp-c$ durch k theilbar ist. Man bemerkt leicht, dass wenn p irgend ein Werth von dieser Beschaffenheit ist, auch $p+wk$, worin w vollkommen willkürlich bleibt, ein solcher sein wird. Demnach gibt es ebenso, wie bei den in §. 75 ff. geführten Untersuchungen, entweder gar keine oder gewisse Reihen der Zahlen von der Form $ap^2-2bp-c$, welche sich sämmtlich herausstellen, wenn man für p nach und nach alle ganzen Zahlen $0, \pm 1, \pm 2, \pm 3 \ldots$ bis hinauf zu derjenigen setzt, welche numerisch $\leqq \frac{k}{2}$ ist. Man findet auch, dass es in Absicht auf die vorliegende Untersuchung nur darauf ankommt, von jeder verschiedenen Reihe Einen Werth von p in Gl. (3) zu substituiren, wozu man also den numerisch kleinsten nehmen kann. Denn eine Substitution von $p+wk$ für p würde keinen andern Effekt haben, als eine Substitution von $z-wy$ für z in Gl. (2).

Wir machen noch darauf aufmerksam, dass sich der Ausdruck (4) in die Form

$$\frac{(ap-b)^2-(b^2+ac)}{ak}$$

oder wenn man $b^2+ac=D$ und $ap-b=P$ setzt, in die Form $-\frac{D-P^2}{ak}=r$ bringen lässt, in welcher derselbe nach §. 75 oder 76 behandelt werden kann, um zuvörderst zulässige Werthe für $P=ap-b$ zu erhalten, welche so beschaffen sein müssen, dass $p=\frac{P+b}{a}$ eine ganze Zahl ist.

Die Gl. (3) hat hiernach die Form

(5) $$ry^2-2Pyz+akz^2=1 .$$

Nachdem hieraus y und z in ganzen Zahlen gefunden sind, ergibt sich nach Gl. (2) auch x als ganze Zahl.

III. Eine der vorstehenden ähnliche Transformation schickt Lagrange der von ihm eingeschlagenen Methode zur Auflösung der im gegenwärtigen Abschnitte behandelten Gleichungen in ganzen Zahlen voraus. (S. dessen Zusätze zu Eulers Algebra.)

Wir müssen darauf Verzicht leisten, jene Methode, womit Lagrange in dem vor seiner Zeit noch wenig kultivirten Gebiete der unbestimmten Analytik die Bahn gebrochen hat, hier ebenfalls noch mitzutheilen, da dieselbe bei ihrer praktischen

Ausführung theils wegen der vorstehenden Transformation, theils wegen der weiteren Rechnungen sich als umständlicher und weniger übersichtlich erweisen dürfte, als die unsrige.

Wir bemerken noch, dass Lagrange nicht für die verschiedenen Fälle, welche sich ergeben, jenachdem die Determinante D positiv und nichtquadratisch, quadratisch, null oder negativ ist, eine einzige, auf demselben Prinzipe beruhende Auflösungsmethode an die Hand gibt, sondern jeden dieser Fälle nach eigenthümlichen Regeln behandelt. Obgleich man in der Praxis in denjenigen Fällen, wo die Determinante quadratisch oder negativ ist, häufig auf einem einfacheren Wege, als nach unserer Methode zum Ziele gelangen kann, wie in §. 121 und 122 gezeigt werden soll; so dürfte diese Methode doch auch hinsichtlich der letzteren Fälle ein bedeutendes wissenschaftliches Interesse aus dem Grunde erwecken, weil sie sich als ein völlig allgemeines Verfahren zur Auflösung der fraglichen Gleichungen erweis't.

Legendre in der *Théorie des nombres* reproduzirt mit geringen Veränderungen die Methoden von Lagrange.

§. 120. *Zerlegung einer Zahl in ihre Primfaktoren und Ermittelung der quadratischen Faktoren einer Zahl.*

I. Die Kenntniss der Faktoren einer Zahl k hat sich bei der Behandlung der unbestimmten Gleichungen vom zweiten Grade schon mehrfach als ein Bedürfniss erwiesen. Namentlich muss man, wenn k die rechte Seite einer solchen Gleichung ist, die quadratischen Faktoren davon kennen, um alle möglichen Auflösungen zu finden.

Das einfachste mechanische Hülfsmittel zur Auffindung dieser Faktoren ist der Gebrauch einer hinreichend ausgedehnten Faktorentafel.

Handelt es sich jedoch um eine wissenschaftliche Auflösung des hierin liegenden Problems nach bestimmten Regeln; so tritt in den Vordergrund das bekannte Verfahren der Versuchsdivisionen mit den sukzessiv höher werdenden Primzahlen. Dieses Verfahren ist durchaus wissenschaftlich, weil es stets nach einer endlichen Menge von bestimmten Operationen zum Ziele führt. Man braucht den Divisor niemals über $\sqrt{k}$ hinaus wachsen zu lassen, um alle verschiedenen Faktoren von k zu erhalten, aus denen sich dann auch leicht alle Primfaktoren von k bestimmen lassen.

Dieses Problem macht übrigens in Wahrheit eine Aufgabe der unbestimmten Analytik aus, da es offenbar darauf ankommt, die unbestimmte Gleichung vom zweiten Grade $xy=k$ in ganzen Zahlen aufzulösen. Dies kann, wenn vorläufig für x und y nur relativ prime Zahlen erwartet werden, nach der obigen Methode geschehen, indem man danach alle je zwei verschiedenen re-

lativ primen Faktoren x, y von k erhält. Ein Beispiel dieser Art ist in §. 113 durchgeführt. Sind also a, b, c, d... verschiedene Primzahlen und $k = 1.a^\alpha b^\beta c^\gamma d^\delta$...; so werden sich folgende Auflösungen in relativ primen Zahlen

$$\begin{array}{llllllll} x = 1 & a^\alpha & b^\beta & \text{etc.} & a^\alpha b^\beta & a^\alpha c^\gamma & \text{etc.} & a^\alpha b^\beta c^\gamma \text{ etc.} \\ y = k & b^\beta c^\gamma \ldots & a^\alpha c^\gamma \ldots & & c^\gamma d^\delta \ldots & b^\beta d^\delta \ldots & & d^\delta \ldots \end{array}$$

ergeben, aus denen man mit Leichtigkeit durch Division mit den kleineren Werthen von x und y in die grösseren die Potenzen der verschiedenen in k enthaltenen Primzahlen a^α, b^β, c^γ... ermitteln wird.

Zur Darstellung der Grössen a^α, b^β. c^γ... kann man auch erst k in irgend zwei Faktoren x, y, alsdann x für sich und y für sich in zwei Faktoren u. s. w. zerlegen, was sich dadurch empfiehlt, dass alsdann die Rechnung immer mehr und mehr auf kleinere Zahlen beschränkt wird.

Es käme dann nur noch auf die Bestimmung der Primzahlen a, b, c... und deren Exponenten α, β, γ... an. Zu diesem Ende wird man aus jeder der Zahlen a^α, b^β, c^γ... die Wurzeln vom Grade 2, 3, 4... ziehen, um nachzusehen, ob z. B. a^α eine höhere Potenz von einer andern Zahl a sein kann, oder ob sie selbst eine Primzahl ist.

Um zu wissen, bis zu welchem Grade diese Wurzelausziehungen höchstens ausgeführt zu werden brauchen, und um die Rechnung möglichst zu vereinfachen, beachte man, dass es stets leicht ist, zu prüfen, ob eine gegebene Zahl a^α durch irgend Eine der Ziffern 2, 3, 4, 5, 6, 7, 8, 9 theilbar sei oder nicht, also auch, ob und welche Potenz sie von 2, 3, 5 oder 7 sei. Angenommen, man habe die gegebene Zahl a^α durch keine der Zahlen 2, 3...10 theilbar gefunden; so kann dieselbe,

wenn sie	$< 11^2$	oder	121	ist,	nur	die	erste
»	» $< 11^3$	»	1331	»	höchstens	die	zweite
»	» $< 11^4$	»	14641	»	»	»	dritte
»	» $< 11^5$	»	161051	»	»	»	vierte

Potenz einer anderen Zahl sein u. s. w.

Um zu zeigen, dass unsere Methode selbst bei grossen Zahlen unter Umständen zu einer ganz einfachen Rechnung führen kann, wollen wir danach die Zahl 9509 in zwei Faktoren zerlegen. Verfährt man nach §. 113; so hat man zu setzen

$$-2xy = -19018.$$

Jetzt sind die Reihen der Zahlen J von der Form $1 - p^2$ zu suchen, welche durch $19018 = 2.9509$ theilbar sind. Wir suchen demnach die durch 9509 theilbaren Zahlen und nehmen daraus diejenigen, welche auch durch 2 theilbar sind (§. 79). Dabei verfahren wir nach §. 77, nehmen also für

r_0 den grössten Subquotienten von $\frac{1}{9509}$, also $r_0 = 0$

r_1 den kleinsten Superquotienten von $\frac{1-\left(\frac{9509-1}{2}\right)^2}{9509}$, also

$$r_1 = -2376$$

Dies gibt folgenden Anfang der Rechnung, worin $D - r_0 q = D = 1$ ist,

r	$\frac{D - rq}{9509 = q}$
$r_0 =$ 0	1
-1	9510
-2	19019
-3	28528
-4	38037
-5	47546
-6	57055
-7	$66564 = 258^2$

Demnach ist für Eine der gesuchten Reihen sehr bald der Werth $p = 258$ gefunden. In dieser Reihe ist nicht das Glied J_{258}, wol aber das nächstfolgende J_{9765}, sowie das nächstzurückliegende J_{9251} auch durch 2, mithin durch 19018 theilbar. Entwickelt man also $K' = \frac{\sqrt{1} + 9251}{19018}$; so kommt

n	P'_n	Q'_n	a'_n
-1		-4500	
0	9251	19018	0
1	-9251	-4500	2
2	251	14	18
3	1	0	-7
4	-1	0	0
5	1	0	

Diese Entwickelung führt erst bei dem Zeiger 3 zu einem Schlusse, in welchem das vorletzte $Q = 14$ ist. Dies würde kein Schluss in kleinsten positiven Zahlen sein. Ein solcher ergibt sich aber nach §. 90 Gl. (1) in vorstehender Weise beim Zeiger 5.

Unter Beachtung der einfachen Entwickelung von $K = \frac{\sqrt{1}+1}{0}$ in §. 113 kann man jetzt $K(1)$ *komb.* $K'(5)$ bilden. Dies gibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	0	0	1
1	0	1	0
2	7	7	1
3	-18	-125	-18
4	-2	257	37

Hiernach ist $x=257$, $y=37$ also $9509=257.37$.

II. Es muss noch darauf aufmerksam gemacht werden, dass nachdem eine durch k theilbare Zahl J von der Form $1-p^2$ gefunden ist, die Faktoren von k auf eine weit einfachere Weise, als vermittelst der vorstehenden Kettenbruchsentwickelung von K und K' dargestellt werden können. Denn nun ist für einen bekannten Werth von p die Grösse $p^2-1=(p+1)(p-1)$ $=rk$, also $k=\frac{(p+1)(p-1)}{r}$. Es ist klar, dass r entweder mit $p+1$ oder mit $p-1$ oder mit beiden ein gemeinschaftliches Maass resp. r' und r'' haben muss, welches sich leicht ermitteln und absondern lässt. Alsdann ergeben sich die Faktoren von k in der Form $k=\frac{p+1}{r'}\cdot\frac{p-1}{r''}$.

Im vorigen Beispiele war für $k=9509$ ein Werth von $p=258$ gefunden, indem man $258^2-1=7.9509$ hat. Dies gibt $9509=\frac{259.257}{7}=\frac{259}{7}.257=37.257$.

III. Man kann jede unpaare Zahl k auch durch Auflösung der Gleichung

$$x^2-y^2=k$$

(s. §. 111) in zwei Faktoren $X=x+y$ und $Y=x-y$ zerlegen. Denn wenn k unpaar ist; so sind je zwei Faktoren X und Y, welche das Produkt k bilden, ebenfalls unpaar. Setzt man also $X=x+y$ und $Y=x-y$; so muss sowol $x=\frac{X+Y}{2}$, als auch $y=\frac{X-Y}{2}$ eine ganze Zahl, mithin $XY=x^2-y^2=k$ in ganzen Zahlen für x und y löslich sein.

Könnte man mit Leichtigkeit eine Quadratzahl y^2 finden, welche, zu k addirt, wiederum eine Quadratzahl x^2 ergäbe; so hätte man sofort Werthe für x, y, welche der Gleichung $x^2=k+y^2$, also auch der obigen $x^2-y^2=k$ genügten, und es wäre sofort für die gesuchten Faktoren $X=x+y$ und $Y=x-y$.

Hierbei muss nothwendig $y\leqq\frac{k-1}{2}$ sein. Dies erhellet, wenn man erwägt, dass in $x^2-y^2=(x+y)(x-y)=k$ stets

$$x+y\leqq k \text{ und } x-y\geqq 1, \text{ also}$$
$$\underline{y-x\leqq -1,} \text{ folglich}$$
$$2y\leqq k-1 \text{ oder } y\leqq\frac{k-1}{2}$$

ist.

Die Auflösung $x=\frac{k+1}{2}$, $y=\frac{k-1}{2}$, welche den Faktoren $X=k$, $Y=1$ entspricht, ist stets möglich. Gibt es ausser

$y = \frac{k-1}{2}$ keine Zahl $< \frac{k-1}{2}$, deren Quadrat, zu k addirt, eine Quadratzahl x^2 hervorbringt; so ist k eine Primzahl. So viel verschiedene y es aber gibt, welche jener Bedingung genügen, in ebenso viel verschiedenen Weisen lässt sich k in zwei Faktoren zerlegen, wobei sowol die negativ primen, wie die mit gemeinschaftlichem Maasse zum Vorschein kommen werden.

Die letzte Methode der Zerlegung einer Zahl in zwei Faktoren ist von Kaussler in dessen Übersetzung der Zusätze von Lagrange zu Eulers Algebra, Anhang II, angegeben.

Da $y = \frac{X-Y}{2}$ ist; so folgt, dass y desto kleiner ist, je kleiner die Differenz zwischen den beiden Faktoren X, Y der Zahl k ist. Die letztere Methode gewährt also da den grössten Vortheil, wo die beiden Faktoren von k möglichst nahe zusammen liegen, also beide zusammen möglichst gross sind. Dies ist aber gerade derjenige Fall, wo die Versuchsdivisionen mit den aufsteigenden Primzahlen die meiste Mühe verursachen würden.

Es sei z. B. $k = 50621$ zu zerlegen. Hier hat man

$$50621 + 0^2 = 50621$$
$$50621 + 1^2 = 50622$$
$$50621 + 2^2 = 50625 = 225^2$$

also $x = 225$, $y = 2$ und demnach

$$X = 225 + 2 = 227, \quad Y = 225 - 2 = 223$$
$$50621 = 227 . 223$$

Die Bildung der Zahlen von der Form $k + y^2$ also k, $k+1$, $k+4$, $k+9$... erleichtert sich mit Hülfe der Differenzreihen, indem man hat

$$k = k$$
$$k + 1 = k + 1$$
$$k + 4 = (k+1) + 3$$
$$k + 9 = (k+4) + 5$$
$$k + 16 = (k+9) + 7$$

IV. Nachdem man alle Primfaktoren einer Zahl k ermittelt hat, kann man mit Leichtigkeit auch alle quadratischen Faktoren von k angeben, welche für die unbestimmten Gleichungen vom zweiten Grade von Wichtigkeit sind.

Diese quadratischen Faktoren lassen sich übrigens durch Versuchsdivisionen in einer ähnlichen Weise finden, wie die einfachen Primfaktoren. Zur Vermeidung unnöthiger Arbeit kann man aber in diesem Falle, wo man vorzugsweise die etwa vorhandenen quadratischen Faktoren darstellen will, folgendes Verfahren einschlagen.

Zuvörderst sieht man nach, ob k selbst ein Quadrat a^2 ist. Bestätigt sich Dies; so nimmt man die Wurzel a und verfährt damit aufs neue wie mit der gegebenen Zahl k.

Bestätigt sich jene Annahme jedoch nicht; so beginnt man mit den aufsteigenden Primzahlen zu dividiren. Sobald eine solche Division aufgeht, also ein Primfaktor von k gefunden ist, sondert man denselben ab, und behandelt den verbleibenden Quotienten wie die gegebene Zahl.

Eine jede Reihe von Versuchsdivisionen mit den aufsteigenden Primzahlen a braucht aber, wenn man nicht schon früher auf einen Faktor des Dividends k stösst, offenbar nur so weit fortgesetzt zu werden, bis der Quotient, welcher sich ergeben würde, wenn man k durch das Quadrat a^2 dividirte, $< a$ werden würde, also nur bis zu derjenigen höchsten Primzahl a, für welche noch $a^2 . a$ oder $a^3 \leqq k$, mithin $a < \sqrt[3]{k}$ ist. Es braucht also,

wenn $k =$	1000	ist,	a	höchstens	$= 7$	zu	sein
»	» =	10000	»	»	»	$= 19$	»	»
»	» =	100000	»	»	»	$= 43$	»	»
»	» =	1000000	»	»	»	$= 97$	»	»

Wäre z. B. $k = 347633$ gegeben; so findet man zunächst, dass k kein vollkommenes Quadrat ist. Die Versuchsdivisionen mit den aufsteigenden Primzahlen lehren, dass k durch 11^2 theilbar ist, und man hat $347633 = 11^2 . 2873$. Jetzt hat man nachzusehen, ob 2873 ein Quadrat sei, was sich nicht bestätigt findet. Die Versuchsdivisionen, bei welchen man mit der Primzahl 11 beginnen kann, lehren dann ferner, dass die letztere Zahl durch 13^2 theilbar und $= 13^2 . 17$ ist. Demnach hat man $347633 = (11 . 13)^2 . 17$.

Wäre $k = 6137$, welches kein Quadrat ist, gegeben; so findet man durch die Versuchsdivisionen zunächst, dass diese Zahl durch 17 theilbar, nämlich $= 17 . 361$ ist. Untersucht man jetzt, ob 361 ein Quadrat sei; so bestätigt sich Dies, indem man $361 = 19^2$ hat. Demnach ist $6137 = 19^2 . 17$.

Wäre $k = 8051$ gegeben; so zeigt sich zuvörderst, dass k kein Quadrat ist. Man findet, dass diese Zahl durch keine der Primzahlen, welche $< \sqrt[3]{8051}$ sind, also durch keine Primzahl bis einschliesslich zur Zahl 19 hinauf, theilbar ist. Demnach kann dieselbe keinen quadratischen Faktor besitzen. Sie ist aber $= 97 . 83$.

§. 121. *Besondere Auflösung der unbestimmten Gleichungen vom zweiten Grade, wenn die Determinante ein Quadrat ist.*

I. Bei der früheren Behandlung dieser Gleichungen assimilirten wir die in der Form

(1) $$ax^2 - 2bxy - cy^2 = k$$
gegebene Gleichung der Beziehung (2) aus §. 68, welche ist
(2) $$Q_0 M_{n-1}^2 - 2P_0 M_{n-1} N_{n-1} - Q_{-1} N_{n-1}^2 = (-1)^n Q_n$$

Wenn die Determinante $D = b^2 + ac$ ein Quadrat ist, und man gestattet die Voraussetzung, dass von jeder gegebenen Zahl sämmtliche Faktoren bekannt seien; so kann man sich mit Vortheil auch der Beziehung (4) aus §. 68 bedienen, welche sich aus der vorstehenden durch Multiplikation mit Q_0 ergibt und
(3) $$(Q_0 M_{n-1} - P_0 N_{n-1})^2 - D N_{n-1}^2 = (-1)^n Q_0 Q_n$$
ist. Multiplizirt man also die gegebene Gleichung (1) mit dem Koeffizienten a und setzt die quadratische Determinante
(4) $$D = b^2 + ac = d^2$$
so kommt
$$(ax - by)^2 - d^2y^2 = ak \text{ oder}$$
(5) $$[ax + (d - b)y]\,[ax - (d + b)y] = ak$$

Sind nun p, q zwei Faktoren, in welche sich die Zahl ak zerlegen lässt, und setzt man
$$ax + (d - b)y = p$$
$$ax - (d + b)y = q$$
so folgt
(6) $$x = \frac{(d + b)p + (d - b)q}{2ad} = \frac{(p + q)d + (p - q)b}{2ad}$$
(7) $$y = \frac{p - q}{2d}$$
wonach auch
(8) $$x = \frac{p + q + 2by}{2a}$$
ist. Man hat also die Zahl ak auf alle mögliche Arten in zwei Faktoren p, q zu zerlegen, die Werthe von p und q in die vorstehenden Werthe von x und y zu substituiren, und dann diejenigen Werthe von x und y beizubehalten, welche ganze Zahlen sind.

Die Faktoren p, q müssen die Grösse ak sowol der Grösse, als auch dem Zeichen nach wiedergeben. Man kann also immer auch die Zeichen von p und q gleichzeitig umkehren. Indessen bemerkt man nach den obigen Werthen von x und y, dass eine Umkehrung der Zeichen von p und q nur einen Zeichenwechsel von x und y zur Folge hat, dass man also die Umkehrung der Zeichen von p und q unterlassen und den Effekt im Resultate darstellen kann. Ist also ak positiv; so braucht man p und q nur positiv zu nehmen: ist dagegen ak negativ; so braucht man nur p positiv und q negativ zu nehmen.

Ferner ist zu beachten, dass nach Gl. (4) statt d auch $-d$ genommen werden kann. Die obigen Ausdrücke für x und y lehren jedoch, dass eine Umkehrung des Zeichens von d den-

selben Erfolg hat, wie eine Verwechselung der beiden Faktoren p und q miteinander. Demnach ist die Umkehrung des Zeichens von d überflüssig, wenn man für p, q alle möglichen numerisch verschiedenen Zerlegungen von ak annimmt.

Beispiel. $3x^2 - 10xy + 7y^2 = 32$.

Hier ist $D = b^2 + ac = 5^2 + 3(-7) = 4 = 2^2$ also $d = 2$. Ferner ist $ak = 3 \,.\, 32 = 96$ mithin

$p =$	96	48	32	24	16	12	8	6	4	3	2	1
$q =$	1	2	3	4	6	8	12	16	24	32	48	96

Zu brauchbaren Auflösungen führen jedoch nur die Zerlegungen $p = 24$, $q = 4$ und $p = 12$, $q = 8$ und man hat hierfür nach Gl. (7) und (8) resp.

$$y = 5,\ 1 \quad \text{also auch} \quad -5,\ -1$$
$$x = 13,\ 5 \qquad\qquad -13,\ -5$$

II. Zu der im gegenwärtigen Paragraphen betrachteten Klasse von Gleichungen gehört stets der Fall, wo die rechte Seite gleich null, also $k = 0$, folglich

$$ax^2 - 2bxy - cy^2 = 0 \tag{9}$$

ist. Da nun $ak = 0$; so ist immer Einer der beiden Faktoren p, q, null und der andere willkürlich. Nimmt man stets $q =$ null und p willkürlich; so muss in den obigen Ausdrücken für x und y die Grösse d zweideutig genommen werden, um alle möglichen Auflösungen zu erhalten. Dies gibt nach Gl. (7) und (6):

$$y = \frac{p}{2d},\quad x = \frac{(d+b)p}{2ad} \tag{10}$$

Hiernach ist zuvörderst, damit y eine ganze Zahl werde, $p = 2dv$ zu setzen, worin v eine willkürliche ganze Zahl bleibt. Dies gibt, wenn man die Zweideutigkeit von d besser markirt,

$$y = v,\quad x = \frac{(\pm d + b)v}{a} \tag{11}$$

Nun muss v so gewählt werden, dass auch x eine ganze Zahl, also $(\pm d + b)v$ ein Vielfaches von a wird. Bezeichnet demnach $\frac{r}{s}$ den auf seine kleinste Benennung gebrachten Bruch $\frac{\pm d + b}{a} = \frac{\pm \sqrt{D} + P_0}{Q_0}$; sodass r und s relativ prim sind; so muss offenbar $v = sw$ also

$$x = rw \qquad y = sw \tag{12}$$

genommen werden, worin w willkürlich bleibt, und wegen der Zweideutigkeit von d jede der beiden Grössen r und s zwei verschiedene Werthe annehmen kann.

Für das Beispiel aus §. 108, wo

$$5x^2 + 8xy - 4y^2 = 0$$

gegeben war, hat man $D=36$, also $d=6$ und

$$\frac{r}{s}=\frac{\pm 6-4}{5}, \text{ d. i. entweder } =\frac{2}{5} \text{ oder } =\frac{-2}{1}$$

Hiernach hat man für r und s die beiden Werthe $r=2$, $s=5$ und $r=-2$, $s=1$, folglich die Auflösungen

$$x=2w, \quad -2w$$
$$y=5w, \quad w$$

III. Ferner gehört hierher der Fall, wo in der gegebenen Gleichung das Quadrat der Einen Unbekannten, etwa das von y, fehlt, also $c=0$ ist. Hiernach hat man $D=d^2=b^2$, also $d=b$ und

(13) $$ax^2-2bxy=k$$

Dies gibt nach den Formeln (6) und (7)

(14) $$x=\frac{p}{a}, \quad y=\frac{p-q}{2b}$$

Hiernach hat man für die Gleichung

$$3x^2-14xy=5$$

aus §. 105 wegen $ak=3.5=15$

$$p=15, \ 5, \ 3, \ 1$$
$$q=1, \ 3, \ 5, \ 15$$

Von diesen Werthen ist nur $p=1$, $q=15$ brauchbar, und Dies gibt $x=5$, $y=1$.

In diesem Falle ist es übrigens nicht nothwendig, dass der Koeffizient des in xy multiplizirten Gliedes eine paare Zahl $2b$ sei. Wäre

(15) $$ax^2+bxy=x(ax+by)=k$$

gegeben; so kann man einfach k in zwei Faktoren p, q zerlegen und

(16) $$x=p, \quad y=\frac{q-ap}{b}$$

setzen, worin y eine ganze Zahl werden muss.

IV. Auch der Fall, wo die Quadrate beider Unbekannten fehlen, wo also $a=0$, $c=0$ und demnach $D=d^2=b^2$ ist, kommt hier in Betracht. Man kann jetzt für die Gleichung $2bxy=k$ einfacher

(17) $$xy=k$$

nehmen. Eine Multiplikation mit $a=0$ würde jedoch hier unstatthaft sein, weil Dies zu der identischen Gleichung $0=0$ führt. Diese Operation ist aber auch unnütz, indem man einfach k in zwei Faktoren p, q zu zerlegen und

(18) $$x=p, \quad y=q$$

zu nehmen hat.

V. Ausserdem gehört zu der obigen Klasse von Gleichungen der Fall, wo das in xy multiplizirte Glied fehlt und zugleich $c=a$, also $ax^2-ay^2=k$ ist. Diese Gleichung kann auf die einfachere Form

(19) $$x^2 - y^2 = k$$
gebracht werden, in welcher man $D = d^2 = 0^2 + 1.1 = 1$, also $d = 1$ hat. Hier ist, wenn $ak = k$ in die beiden Faktoren p, q zerlegt ist, nach Gl. (6) und (7)

(20) $$x = \frac{p+q}{2} \qquad y = \frac{p-q}{2}$$
sodass nur die Summe und die Differenz der beiden Faktoren p, q paare Zahlen zu sein brauchen.

Wäre z. B. $x^2 - y^2 = 24$ gegeben; so hätte man

$p = 24 \quad 12 \quad 8 \quad 6 \quad 4 \quad 3 \quad 2 \quad 1$
$q = 1 \quad 2 \quad 3 \quad 4 \quad 6 \quad 8 \quad 12 \quad 24$

Hier sind nur die Werthe

$p = 12 \quad 6 \quad 4 \quad 2$
$q = 2 \quad 4 \quad 6 \quad 12$

brauchbar, und ergeben die Auflösungen

$x = 7 \quad 5 \quad 5 \quad 7$
$y = 5 \quad 1 \quad -1 \quad -5$

welche noch mit entgegengesetzten Zeichen genommen werden können.

VI. Endlich ist hier der Fall zu betrachten, wo die Determinante D, also auch d gleich null ist. Dieser Fall hat aber das Eigenthümliche, dass nun die beiden Faktoren auf der linken Seite der Gl. (5) einander gleich, also
$$ax - by = p = q$$
sein muss. Hieraus folgt, dass die Zahl ak in zwei gleiche Faktoren p, q zu zerlegen ist, und Dies setzt mit Nothwendigkeit voraus, dass ak ein vollständiges Quadrat sei. Wir haben aber schon in §. 114 gesehen, dass wenn die vier Koeffizienten a, $2b$, c, k von ihrem gemeinschaftlichen Maasse befreiet sind, sowol a, wie auch k für sich allein ein Quadrat sein muss, sodass also die gegebene Gleichung in die Form

(21) $$f^2x^2 - 2fgxy + g^2y^2 = (fx - gy)^2 = k^2$$
gestellt werden kann und in die beiden Gleichungen

(22) $$fx - gy = \pm k$$
vom ersten Grade zerfällt.

§. 122. *Besondere Auflösung der unbestimmten Gleichungen vom zweiten Grade, wenn die Determinante negativ ist.*

Auch unter diesen Umständen, wo die Determinante negativ ist, wo man also

(1) $$-D = b^2 + ac$$
schreiben kann, lässt sich die gegebene Gleichung

(2) $$ax^2 - 2bxy - cy^2 = k$$
nachdem man dieselbe mit a multiplizirt hat, in der Form der Gl. (3) des vorhergehenden Paragraphen behandeln. Man hat alsdann

(3) $$(ax - by)^2 + Dy^2 = ak$$

Da die linke Seite positiv ist, muss es auch die rechte ak sein, was auch schon in §. 115 bemerkt ist. Da $(ax - by)^2$ nicht negativ werden kann; so kann Dy^2 den Werth ak nicht übersteigen; es muss also sein

(4) $$Dy^2 \leqq ak, \text{ folglich } y \leqq \sqrt{\frac{ak}{D}}$$

Durch Transposition wird nun die Gl. (3), indem man zur Abkürzung

(5) $$ax - by = z, \text{ folglich}$$

(6) $$x = \frac{z + by}{a} \text{ setzt,}$$

(7) $$ak - Dy^2 = z^2$$

Hiernach substituire man in die linke Seite der Gl. (6) für y alle positiven ganzen Zahlen von 0 bis $\sqrt{\frac{ak}{D}}$ und ermittele diejenigen, für welche diese linke Seite ein vollkommenes Quadrat z^2 wird. Jeden für z gefundenen Werth setze man in Gl. (6) und behalte nur diejenigen bei, für welche x eine ganze Zahl wird. Hierdurch ergeben sich alle zusammengehörigen Werthe von x, y, welche Auflösungen der gegebenen Gleichung (2) bilden. Man hat aber zu beachten, dass jeder zulässige Werth von z und y für sich sowol positiv, wie negativ genommen werden kann.

Beispiel 1. $3x^2 - 10xy + 11y^2 = 27$

In diesem schon in §. 115 behandelten Beispiele hat man $-D = -8$ und statt Gl. (7)

$$81 - 8y^2 = z^2$$

Hier sind für y alle ganzen Zahlen bis zu $\sqrt{\frac{81}{8}}$ also bis 3 zu setzen. Dies gibt

$$81 - 8 . 0^2 = 81 = 9^2$$
$$81 - 8 . 1^2 = 73$$
$$81 - 8 . 2^2 = 49 = 7^2$$
$$81 - 8 . 3^2 = 9 = 3^2$$

Von den hieraus folgenden Werthen $0, \pm 2, \pm 3$ für y, welche resp. den Werthen $\pm 9, \pm 7, \pm 3$ für z entsprechen, wobei jedoch die Zeichen von y und die von z unabhängig und willkürlich sind, hat man diejenigen beizubehalten, für welche nach Gl. (6) $x = \frac{z + 5y}{3}$ eine ganze Zahl wird. Dies liefert folgende Auflösungen

$$x = 3 \quad -3 \quad 1 \quad -1 \quad 6 \quad 4 \quad -6 \quad -4$$
$$y = 0 \quad 0 \quad 2 \quad -2 \quad 3 \quad 3 \quad -3 \quad -3$$

welche auch in §. 115 gefunden sind.

Beispiel 2. Zu der vorstehenden Klasse von Gleichungen gehört immer der Fall, wo das in xy multiplizirte Glied fehlt, (also $b=0$ ist) und a und c ungleiche oder a und $-c$ gleiche Zeichen haben, also insofern man mit a, c', k drei positive Zahlen bezeichnet, die Gleichung

(8) $$ax^2+c'y^2=k$$

Eine Spezialität dieser Gleichung ist

(9) $$x^2+y^2=k$$

Hier ist $-D=0^2+1\,(-1)=-1$ und statt Gl. (7) hat man

(10) $$k-y^2=x^2$$

indem nach Gl. (6) $z=x$ stets eine ganze Zahl ist.

Wäre z. B.

$$x^2+y^2=41$$

gegeben; so muss $y \leqq \sqrt{41}$, also $\leqq 6$ sein. Demnach hat man

$$41-0^2=41$$
$$41-1^2=40$$
$$41-2^2=37$$
$$41-3^2=32$$
$$41-4^2=25=5^2$$
$$41-5^2=16=4^2$$
$$41-6^2=\ \ 5$$

folglich $x=\pm 5,\ \pm 4$
$y=\pm 4,\ \pm 5$

worin die Zeichen der korrespondirenden Werthe von x und y willkürlich genommen werden können.

§. 123. *Independente Formeln für die Auflösungen der unbestimmten Gleichungen vom zweiten Grade mit positiver nicht quadratischer Determinante.*

I. Für den Fall, wo die Determinante positiv und nicht quadratisch ist, wo es also eine unendliche Menge von Auflösungen gibt, sind zuweilen independente Ausdrücke für diese Auflösungen von Interesse. Nach §. 100 gruppiren sich diese Auflösungen in Reihen, welche sich nach beiden Seiten ins Unendliche fortsetzen. Die Glieder einer solchen Reihe sind dargestellt durch

$$x=\ldots\overset{-n}{M}\ldots\overset{-2}{M}\ \overset{-1}{M}\ \overset{0}{M}\ \overset{1}{M}\ \overset{2}{M}\ldots\overset{n}{M}\ldots$$
$$y=\ldots\overset{-n}{N}\ldots\overset{-2}{N}\ \overset{-1}{N}\ \overset{0}{N}\ \overset{1}{N}\ \overset{2}{N}\ldots\overset{n}{N}\ldots$$

Angenommen, zwei benachbarte Auflösungen dieser Reihe, nämlich

$$x=\overset{0}{M}\quad\overset{1}{M}$$
$$y=\overset{0}{N}\quad\overset{1}{N}$$

seien nach den Regeln des §. 100 berechnet, auch sei die dort und in §. 82 bis 85 mit h bezeichnete Grösse bestimmt.

Nach der betreffenden Bemerkung in §. 100 hat diejenige Periode, welche bei der Kombinirung von K und K' in Betracht kommt, stets eine paare Menge r von Gliedern, sodass $(-1)^r = 1$ und $(-1)^{r-1} = -1$ ist, und demzufolge die in §. 85 mit $h_0, h_1, h_2 \ldots$ bezeichneten Grössen nach dem Subtraktionsprinzipe gebildet sind. Demgemäss hat man nach Gl. (2) in §. 85 hier immer

$$(1) \qquad h_n = h^n - \overset{n-1}{B_1} h^{n-2} + \overset{n-2}{B_2} h^{n-4} - \overset{n-3}{B_3} h^{n-6} + \text{etc.}$$

Diese Reihe setzt sich, jenachdem n paar oder unpaar ist, so weit fort, bis der Exponent von h resp. $= 1$ oder $= 0$ wird.

Nun hat man nach §. 85 Gl. (9) unter der Bedingung, dass n positiv sei,

$$(2) \qquad \begin{cases} x = \overset{n}{M} = h_{n-1} \overset{1}{M} - h_{n-2} \overset{0}{M} \\ y = \overset{n}{N} = h_{n-1} \overset{1}{N} - h_{n-2} \overset{0}{N} \end{cases}$$

Für die rückwärts in der fraglichen Reihe liegenden Auflösungen hat man

$$(3) \qquad \begin{cases} x = \overset{-n}{M} = h_n \overset{0}{M} - h_{n-1} \overset{1}{M} \\ y = \overset{-n}{N} = h_n \overset{0}{N} - h_{n-1} \overset{1}{N} \end{cases}$$

Substituirt man hierin für h_n, h_{n-1}, h_{n-2} ihre Ausdrücke nach dem Gesetze (1); so hat man einen independenten Ausdruck für die in der fraglichen Reihe vorwärts und für die rückwärts liegenden Auflösungen.

II. Wir dürfen nicht unterlassen, eine beachtenswerthe independente Formel von Lagrange (Zusätze zu Eulers Algebra §. 75) für die Auflösungen der einfacheren Gleichung

$$(4) \qquad x^2 - Dy^2 = 1$$

mitzutheilen. Dieselbe wird folgendermaassen gewonnen. Es sei X, Y eine bereits gefundene Auflösung, (jedoch nicht die Auflösung $X = 1$, $Y = 0$) also $X^2 - DY^2 = 1$. Wäre nun X', Y' eine zweite Auflösung, also auch $X'^2 - DY'^2 = 1$; so ist, wenn man diese beiden Gleichungen miteinander multiplizirt und gehörig reduzirt,

$$(5) \quad (X^2 - DY^2)(X'^2 - DY'^2) = (XX' + DYY')^2 - D(XY' + YX')^2 = 1$$

Hieraus folgt, dass nun auch

$$(6) \qquad \begin{cases} x = XX' + DYY' \\ y = XY' + YX' \end{cases}$$

eine Auflösung der gegebenen Gleichung sein wird.

Um hieraus einen independenten Ausdruck für x, y abzuleiten, beachte man, dass wenn man den Werth von y mit $\sqrt{D}$

multiplizirt und Einmal zu x addirt, Einmal aber davon subtrahirt, man die Beziehungen

(7) $$x + y\sqrt{D} = (X + Y\sqrt{D})(X' + Y'\sqrt{D})$$

(8) $$x - y\sqrt{D} = (X - Y\sqrt{D})(X' - Y'\sqrt{D})$$

erhält.

Setzt man also in die Formeln (6) für X', Y' die ursprüngliche Auflösung X, Y, dann in dieselben Formeln für X', Y' die für x, y gefundene neue Auflösung, dann in die nämlichen Formeln für X', Y' die zuletzt für x, y sich ergebende Auflösung und so fort; so sind die sukzessiv für x, y zum Vorschein kommenden Werthe von der Art, dass sie statt der Beziehungen (7), (8) die folgenden ergeben,

(9) $$x + y\sqrt{D} = (X + Y\sqrt{D})^n$$

(10) $$x - y\sqrt{D} = (X - Y\sqrt{D})^n$$

worin man für n jede positive ganze Zahl setzen kann.

Aus (9) und (10) erhält man die nachstehenden independenten Ausdrücke für x, y

(11) $$\begin{cases} x = \dfrac{(X + Y\sqrt{D})^n + (X - Y\sqrt{D})^n}{2} \\[2ex] y = \dfrac{(X + Y\sqrt{D})^n - (X - Y\sqrt{D})^n}{2\sqrt{D}} \end{cases}$$

Diese Ausdrücke liefern für x und y stets ganze Werthe, wovon man sich durch Entwickelung der Potenzen der Binome überzeugen kann.

Dass diese Formeln übrigens nur dann brauchbar sind, wenn die Determinante D positiv und nicht quadratisch ist, leuchtet ein. Denn wäre sie quadratisch; so kann sie nur $= 1$ sein, weil für keinen anderen Werth von $D = d^2$ die Gleichung $x^2 - d^2y^2 = (x + dy)(x - dy) = 1$ bestehen kann. Ist aber $D = 1$; so wird nothwendig $X = 1$, $Y = 0$ sein müssen, und daraus folgt nach (11) auch allgemein $x = 1$, $y = 0$.

Wäre dagegen D negativ $= -D$; so könnte die Gleichung $X^2 + DY^2 = 1$ ebenfalls nur für $X = 1$, $Y = 0$ bestehen, was auch die allgemeine Auflösung $x = 1$, $y = 0$ nach sich zieht.

Lagrange hat gezeigt, dass wenn X, Y die Auflösung der gegebenen Gleichung in absolut kleinsten Zahlen ist, (jedoch nicht die Auflösung $X = 1$, $Y = 0$) die allgemeine Formel (11) alle möglichen Auflösungen der gegebenen Gl. (4) ergibt, sobald man n in der Reihe der Zahlen 0, 1, 2, 3... variiren lässt. Man kann übrigens in jeder Auflösung x, y sowol x, wie auch y mit beliebigen Zeichen nehmen. Ein Wechsel der Zeichen der in (11) zu substituirenden ursprünglichen Grössen X und Y kann offenbar keine Auflösungen liefern, welche numerisch von den früheren verschieden wären.

Demnach kann man X und Y als positiv voraussetzen und sich den Zeichenwechsel von x und y vorbehalten.

§. 124. Transformation, Äquivalenz und Reduktion der quadratischen Formen.

I. Für verschiedene Zwecke ist es wichtig, zu untersuchen, durch welche verschiedene, einer gegebenen Determinante angehörige quadratische Formen Ein und dieselbe Grösse k sich darstellen lasse, welche Werthe man also in der Gleichung

(1) $$ax^2 - 2bxy - cy^2 = k$$

für die Zahlen a, b, c setzen könne, sodass die linke Seite immer fähig ist, für gewisse ganze Werthe von x und y die Grösse k darzustellen.

Assimilirt man zu diesem Zwecke die gegebene Gleichung der bekannten Beziehung (2) aus §. 68

(2) $Q_0 M_{n-1}^2 - 2P_0 M_{n-1} N_{n-1} - Q_{-1} N_{n-1}^2 = (-1)^n Q_n$ oder

(3) $Q_0 x^2 - 2P_0 xy - Q_{-1} y^2 = (-1)^n Q_n = k$

und entwickelt nun die Grösse

(4) $$K = \frac{\sqrt{D} + P_0}{Q_0} = \frac{\sqrt{b^2 + ac} + b}{a}$$

in einen Kettenbruch, wobei man die Quotienten a_0, a_1, $a_2 \ldots$ ganz beliebig annehmen kann; so hat man, wenn man beachtet, dass man jedes spätere Glied dieser Entwickelung *als* das erste betrachten kann,

$$Q_0 x^2 - 2P_0 x y - Q_{-1} y^2 = (-1)^n Q_n = k \text{ und}$$
$$\frac{x}{y} = [a_0, a_1, a_2, a_3 \ldots a_{n-1}]$$
$$Q_1 x_1^2 - 2P_1 x_1 y_1 - Q_0 y_1^2 = (-1)^{n-1} Q_n = -k \text{ und}$$
$$\frac{x_1}{y_1} = [a_1, a_2, a_3 \ldots a_{n-1}]$$
$$Q_2 x_2^2 - 2P_2 x_2 y_2 - Q_1 y_2^2 = (-1)^{n-2} Q_- = k \text{ und}$$
$$\frac{x_2}{y_2} = [a_2, a_3 \ldots a_{n-1}]$$
$$Q_3 x_3^2 - 2P_3 x_3 y_3 - Q_2 y_3^2 = (-1)^{n-3} Q_n = -k \text{ und}$$
$$\frac{x_3}{y_3} = [a_3 \ldots a_{n-1}]$$

etc. etc. etc.

(5) $$\begin{cases} Q_m x_m^2 - 2P_m x_m y_m - Q_{m-1} y_m^2 = (-1)^{n-m} Q_n = (-1)^m k \text{ und} \\ \dfrac{x_m}{y_m} = [a_m, a_{m+1} \ldots a_{n-1}] \end{cases}$$

So ist z. B. für $3x^2 - 10xy - 4y^2 = 7$, indem hier $K = \frac{\sqrt{37} + 5}{3}$ folgende Entwickelung liefert

n	P_n	Q_n	$(-1)^n Q_n$	a_n
-2				
-1		4	-4	
0	5	3	3	3
1	4	7	-7	1
2	3	4	4	2
3	5	3	-3	3
4	4	7	7	1
5	3	4	-4	2

$$3x^2 - 10xy - 4y^2 = 7 \text{ und } \frac{x}{y} = [3, 1, 2, 3] = \frac{37}{10}$$

$$7x_1^2 - 8x_1y_1 - 3y_1^2 = -7 \text{ und } \frac{x_1}{y_1} = [1, 2, 3] = \frac{10}{7}$$

$$4x_2^2 - 6x_2y_2 - 7y_2^2 = 7 \text{ und } \frac{x_2}{y_2} = [2, 3] = \frac{7}{3}$$

$$3x_3^2 - 10x_3y_3 - 4y_3^2 = -7 \text{ und } \frac{x_3}{y_3} = [3] = \frac{3}{1}$$

II. Was die Beziehung zwischen den Grössen x, y in der ursprünglich gegebenen und den Grössen x_m, y_m in einer späteren transformirten Gleichung anlangt; so hat man

(6) $$[a_0, a_1, a_2 \ldots a_{m-1}] = \frac{M_{m-1}}{N_{m-1}}$$

(7) $$[a_0, a_1, a_2 \ldots a_{n-1}] = \frac{M_{n-1}}{N_{n-1}} = \frac{x}{y}$$

(8) $$[a_m, a_{m+1}, a_{m+2} \ldots a_{n-1}] = \frac{\mathfrak{M}_{n-m-1}}{\mathfrak{N}_{n-m-1}} = \frac{x_m}{y_m}$$

also sofort nach §. 15

(9) $$x = M_{m-1}x_m + M_{m-2}y_m$$

(10) $$y = N_{m-1}x_m + N_{m-2}y_m$$

Hieraus folgt auch

(11) $x_m = (-1)^{m-2}(N_{m-2}x - M_{m-2}y)$ oder $\pm x_m = N_{m-2}x - M_{m-2}y$

(12) $y_m = (-1)^{m-1}(N_{m-1}x - M_{m-1}y)$ $\quad\mp y_m = N_{m-1}x - M_{m-1}y$

Wenn also x, y ganze Zahlen sind, so müssen auch nothwendig x_m, y_m es sein, und umgekehrt. Diese Beziehung ist eine Folge der Bedingung

(13) $$M_{m-1}N_{m-2} - M_{m-2}N_{m-1} = (-1)^{m-1}$$

welcher die vier Koeffizienten M_{m-2}, N_{m-2}, M_{m-1}, N_{m-1} genügen müssen.

III. Multipliziren wir in der Reihe der sub I. aufgeführten quadratischen Formen die 2te, 4te, 6te ... mit -1; so nehmen dieselben folgende Gestalt an

$$Q_0x^2 - 2P_0xy - Q_{-1}y^2 = (-1)^n Q_n = k$$
$$-Q_1x_1^2 + 2P_1x_1y_1 + Q_0y_1^2 = (-1)^n Q_n = k$$
$$Q_2x_2^2 - 2P_2x_2y_2 - Q_1y_2^2 = (-1)^n Q_n = k$$
$$-Q_3x_3^2 + 2P_3x_3y_3 + Q_2y_3^2 = (-1)^n Q_n = k$$

. . . .

(14) $$(-1)^m Q_m x_m^2 - 2(-1)^m P_m x_m y_m - (-1)^m Q_{m-1} y_m^2 = (-1)^n Q_n = k$$

Hierin behalten die Unbekannten genau die früheren Werthe und gegenseitigen Beziehungen. Die rechten Seiten wechseln aber nicht mehr das Zeichen, sondern behalten fortwährend Ein und denselben Werth $(-1)^n Q_n = k$. Demnach besteht die wesentliche Beziehung zwischen irgend zwei dieser Formen, etwa zwischen der ersten und der letzten (14) in Folgendem.

Die erste Form geht in die letzte über, indem man für ihre Unbekannten x, y Ausdrücke von der Zusammensetzung der Formeln (9), (10) substituirt, welche in Beziehung zu den neuen Unbekannten x_m, y_m lineär und mit ganzen Koeffizienten behaftet sind. Durch eine ganz ähnliche Substitution geht aber auch vermöge der Formeln (11), (12) die letzte Form in die erste über.

Diese Eigenschaft läuft auch darauf hinaus, dass jede Zahl k, welche sich für ganze Werthe der Unbekannten durch die Eine Form darstellen lässt, ebenso auch durch die andere Form dargestellt werden kann.

Formen von dieser Beschaffenheit heissen äquivalent, und man sagt auch, dass die Eine in der anderen enthalten sei.

IV. Es lässt sich ohne Schwierigkeit zeigen, dass Formen, welche äquivalent sein sollen, nothwendig nicht bloss *dieselbe* Determinante besitzen, sondern auch, wie die vorstehende Reihe von Formen, der Kettenbruchsentwickelung Ein und derselben Grösse K angehören müssen. Denn substituirt man in die erste Form allgemein Werthe von der Form

(15) $$x = \alpha x_m + \beta y_m$$

(16) $$y = \gamma x_m + \delta y_m$$

so entsteht eine neue Form, deren Determinante, wenn man zur Abkürzung $\alpha\delta - \beta\gamma = e$ setzt,

(17) $$D' = De^2$$

ist, und aus den Gleichungen (15) folgt zugleich

(18) $$e x_m = \delta x - \beta y$$

(19) $$-e y_m = \gamma x - \alpha y$$

Soll nun umgekehrt durch eine analoge Substitution für x_m, y_m die zweite Form auch in die erste verwandelt werden können; so muss, da durch diese Substitution eine Form von der Determinante $D' e'^2 = De^2 e'^2$ entsteht, worin auch e' eine ganze Zahl ist, $De^2 e'^2 = D$ also $e^2 = e'^2 = 1$, folglich

(20) $$e = \alpha\delta - \beta\gamma = \pm 1$$

und demnach auch $D' = D$ sein. Die Bedingung $e = \pm 1$ hat dann auch zur Folge, dass wegen der Gleichungen (18), (19) für alle ganzen Werthe von x, y auch x_m, y_m ganze Zahlen werden.

Hieraus ist klar, dass die Determinanten beider äquivalenten Formen einander gleich und dass die Koeffizienten α, γ, β, δ resp. als M_{m-1}, N_{m-1}, M_{m-2}, N_{m-2} die Zähler und Nenner zweier benachbarter Näherungswerthe Ein und desselben Kettenbruchs repräsentiren, wodurch die Formeln (15), (16), (18), (19), (20) resp. mit den früheren (9), (10), (11), (12), (13) identisch werden.

V. Sind nun die beiden gegebenen Formen

(21) $$a\,x^2 - 2bxy - cy^2$$

(22) $$a'\,x'^2 - 2b'x'y' - c'y'^2$$

deren Determinanten $b^2 + ac = b'^2 + a'c' = D$ einander gleich seien; so erfordert die Äquivalenz beider, dass wenn man die aus der ersten Form abgeleitete Grösse $K = \frac{\sqrt{D} + b}{a}$ in einen Kettenbruch mit irgend welchen Quotienten entwickelt und die nach der Formel (5) gebildeten Formen aufstellt, die zweite äquivalente Form entweder mit denselben Koeffizienten a', b', c' bei einem paaren Zeiger m oder mit entgegengesetzten Koeffizienten $-a'$, $-b'$, $-c'$, also in der Gestalt $-a'\,x'^2 + 2b'\,x'\,y' + c'\,y'^2$, bei einem unpaaren Zeiger m erscheine. Dies ergibt folgendes Verfahren zur Prüfung der Äquivalenz der beiden Formen (21), (22).

Man entwickelt die aus der ersten Form genommene Grösse $K = \frac{\sqrt{D} + b}{a}$ in einen Kettenbruch mit grössten Subquotienten und zwar, wenn D positiv und kein Quadrat ist, mit der von selbst sich einstellenden Periode, wenn D aber negativ ist, mit der Periode in kleinsten positiven Zahlen, und wenn D ein positives Quadrat ist, mit dem Schlusse in kleinsten positiven Zahlen.

Entwickelt man hierauf sowol die aus der zweiten Form abgeleitete Grösse $K' = \frac{\sqrt{D} + b'}{a'}$, als auch die aus der zweiten Form mit entgegengesetzten Koeffizienten abgeleitete Grösse $K'' = \frac{\sqrt{D} - b'}{-a'}$ in derselben Weise in einen Kettenbruch; so muss, wenn die beiden gegebenen Formen (21), (22) äquivalent sein sollen, entweder die Periode, resp. der Schluss, von K' mit der Periode, resp. dem Schlusse, von K dergestalt übereinstimmen, dass die Zeigersumme der übereinstimmenden Glieder paar ist, oder es muss die Periode, resp. der Schluss, von K'' mit der Periode, resp. dem Schlusse, von K dergestalt übereinstimmen, dass die Zeigersumme der über-

einstimmenden Glieder unpaar ist. Im ersteren Falle, wo also auch m paar, folglich $(-1)^{m-1} = -1$, also wegen der Beziehungen (13) und (20) die Grösse $e = -1$ ist, würden wir die beiden Formen eigentlich äquivalent, im letzteren Falle dagegen, wo m unpaar und $e = +1$ ist, uneigentlich äquivalent nennen, wogegen Gauss in den *Disq. arithm.* 157, 158 die umgekehrte Benennung eingeführt hat, was darin seinen Grund haben dürfte, dass daselbst die quadratischen Formen nicht in der vorstehend erläuterten Beziehung zu den Kettenbrüchen betrachtet sind. Zwei Formen können übrigens sowol in der Einen, wie in der anderen Weise äquivalent sein.

Wenn man beachtet, dass nach §. 71 die Perioden der Grössen $K'' = \frac{\sqrt{D} - b'}{-a'}$ und $\frac{\sqrt{D} - b'}{a'}$ identisch sind, so jedoch, dass die Differenz oder auch die Summe der übereinstimmenden Glieder unpaar ist; so kann man auch über die Äquivalenz der beiden Formen (21), (22) dadurch entscheiden, dass man jede der durch $\frac{\sqrt{D} \pm b'}{a'}$ dargestellten beiden Grössen entwickelt und nachsieht, ob die Periode, resp. der Schluss, irgend Einer derselben mit der Periode, resp. dem Schlusse von K dergestalt übereinstimmt, dass die Zeigersumme der übereinstimmenden Glieder paar ist.

Bei dieser Untersuchung ist auch die Rücksicht auf den Nachtrag zu §. 72 am Ende des vierten Abschnittes nützlich, wonach die Periode der Einen der beiden Grössen $\frac{\sqrt{D} + b'}{a'}$ und $\frac{\sqrt{D} - b'}{-a'}$ das Umgekehrte von der der anderen ist, woraus sich, wenn die beiden Formen (21), (22) nicht äquivalent sind, die Unmöglichkeit der Äquivalenz oftmals schon dann erkennen lässt, nachdem man die erste dieser beiden Grössen entwickelt hat.

VI. Um eine Form (21) in die ihr äquivalente (22) zu transformiren, hat man offenbar die Entwickelung von K mit der Entwickelung von K' oder K'' zu kombiniren, indem man der in §. 73 auf Seite 179 dargestellten Kombination schliesslich noch den Quotienten 0 hinzufügt, wodurch offenbar der Schluss

$$P'_0, \quad Q'_0, \quad Q'_{-1}$$

entsteht, welcher, wenn die Kombination mit K' stattgefunden hat, sofort die zweite Form (22) bei paarem Zeiger, oder wenn die Kombination mit K'' stattgefunden hat, die Form $-a'x'^2 + 2b'x'y' + c'y'^2$ bei unpaarem Zeiger, welche

durch Umkehrung der Zeichen ebenfalls in die Form (22) übergeht, darstellt.

Um z. B. die der Determinante 37 angehörigen beiden Formen $3x^2 - 10xy - 4y^2$ und $4x'^2 + 2x'y' - 9y'^2$ auf ihre Äquivalenz zu prüfen und alsdann die Transformation der ersten in die zweite zu bewirken, haben wir

$$K = \frac{\sqrt{37}+5}{3} \qquad K' = \frac{\sqrt{37}-1}{4}$$

n	P_n	Q_n	a_n	n	P'_n	Q'_n	a'_n
-1		4		-1		9	
0	5	3	3	0	-1	4	1
1	4	7	1	1	5	3	3
2	3	4	2	2	4	7	1
3	5	3	3	3	3	4	2
4	4	7	1				
	etc.				etc.		

Die Perioden von K und K' stimmen, wenn man dieselben resp. von den Zeigern 4 und 2 an rechnet, so überein, dass die Zeigersumme der übereinstimmenden Glieder paar ist. Die beiden gegebenen Formen sind also äquivalent, und zwar eigentlich äquivalent. Da die Periode nicht symmetrisch ist; so kann die Periode von $K'' = \frac{\sqrt{37}+1}{-4}$ nicht mit der von K übereinstimmen: die beiden gegebenen Formen können also nicht zugleich auch uneigentlich äquivalent sein.

Um von den unendlich vielen verschiedenen Transformationen der ersten Form in die zweite die der Kombination $K(4)$ *komb.* $K'(2)$ entsprechende zu bilden; so hat man

m	P_m	Q_m	a_m	M_m	N_m
-2				0	1
-1		4		1	0
0	5	3	3	3	1
1	4	7	1	4	1
2	3	4	2	11	3
3	5	3	3	37	10
4	4	7	0	11	3
5	-4	3	-3	4	1
6	-5	4	-1	7	2
7	1	9	0	4	1
8	-1	4			

wodurch also die zweite Form als ein Glied der Entwickelung der ersten Form bei dem paaren Zeiger $m = 8$ erscheint.

Da man hiernach $M_{m-1} = 4$, $N_{m-1} = 1$, $M_{m-2} = 7$, $N_{m-2} = 2$ hat; so ist nach den Formeln (9), (10) die Substitution, wodurch die erste Form in die zweite übergeht

$$x = 4x' + 7y'$$
$$y = 1x' + 2y'$$

VII. Aus den gegenwärtigen Beziehungen und den Ge-

setzen des vierten Abschnittes, namentlich aus §. 71, 72 und dem Nachtrage zu §. 72 am Ende des vierten Abschnittes erkennt man leicht, dass wenn man die Form

$$ax^2 - 2bxy - cy^2 \text{ kurz mit } (a,\ b,\ c)$$

bezeichnet, die vier Formen

$$(a,\ b,\ c),\ (a,\ -b,\ c),\ (-c,\ b,\ -a),\ (-c,\ -b,\ -a)$$

einander äquivalent sind.

Ferner erkennt man, dass wenn die Periode von (a, b, c) eine unpaare Gliederzahl besitzt, die Form (a, b, c) auch äquivalent der Form $(-a, -b, -c)$ und demnach auch äquivalent den Formen $(-a, b, -c)$, $(c, -b, a)$, (c, b, a) ist.

VIII. Die Untersuchungen des vierten Abschnittes lehren ferner Folgendes.

Wenn die Determinante D positiv und kein Quadrat ist; so sind in der Periode des Ausdrucks K die Grössen P_m, Q_m, Q_{m-1} positiv, es ist $P_m < \sqrt{D}$ und sowol Q_m, als auch $Q_{m-1} < 2\sqrt{D}$.

Wenn die Determinante negativ $= -D$ ist; so hat man für die Periode in kleinsten Zahlen, absolut genommen, $P_m \leqq \frac{D-1}{2}$, $Q_m \leqq \frac{D+1}{2}$ und $Q_m Q_{m-1} \leqq \left(\frac{D+1}{2}\right)^2$, indem Q_m und Q_{m-1} entgegengesetzte Zeichen annehmen.

Wenn die Determinante ein positives Quadrat $= d^2$ ist; so hat man für den Schluss in kleinsten positiven Zahlen $P_m = d$, $Q_m = 0$, Q_{m-1} positiv und $\leqq d$.

Wenn die Determinante gleich null ist, wird $P_m = 0$, $Q_m = 0$, Q_{m-1} positiv und gleich dem grössten gemeinschaftlichen Maasse, welches die drei Zahlen a, b, c in der gegebenen und in jeder ihr äquivalenten Form besitzen.

IX. Noch wichtiger für die Transformation der quadratischen Formen ist das nachstehende Gesetz. Wenn man die Grösse K für eine positive nicht quadratische Determinante nach §. 69 und für eine negative Determinante nach §. 97 in eine zweigliedrige Periode entwickelt; so wird, absolut genommen, $P_m \leqq \frac{1}{2} Q_m$ und auch $\leqq \frac{1}{2} Q_{m-1}$ sein, es wird also in der neuen Form (14) der absolute Werth des mittleren Koeffizienten $2P_m$ keinen der beiden äussern Koeffizienten Q_m und Q_{m-1} übersteigen.

Ausserdem aber wird,

wenn die Determinante D positiv und kein Quadrat *ist*, absolut $P_m \leqq \sqrt{\frac{D}{5}}$ und nach Belieben entweder Q_m oder Q_{m-1} absolut $\leqq \sqrt{D}$ sein, wobei Q_m und Q_{m-1} gleiche Zeichen, also die beiden äusseren Glieder der Form (14) entgegensetzte Zeichen besitzen.

Wenn dagegen die Determinante negativ $= -D$ ist, wird absolut $P_m \leqq \sqrt{\frac{D}{3}}$ und nach Belieben entweder Q_m oder Q_{m-1} absolut $\leqq \sqrt{\frac{4D}{3}}$ sein, wobei Q_m und Q_{m-1} entgegengesetzte Zeichen, also die beiden äusseren Glieder der Form (14) gleiche Zeichen besitzen.

Ist die Determinante ein positives Quadrat $= d^2$; so hat man für den Schluss in kleinsten positiven Zahlen, wie schon vorhin erwähnt, $P_m = d$, $Q_m = 0$, Q_{m-1} positiv und $\leqq d$.

Wenn die Determinante gleich null ist, wird $P_m = 0$, $Q_m = 0$, Q_{m-1} positiv und gleich dem grössten gemeinschaftlichen Maasse, welches die drei Zahlen a, b, c in der gegebenen und in jeder ihr äquivalenten Form besitzen.

Eine Form, deren Koeffizienten der betreffenden der eben genannten Bedingungen entsprechen, heisst eine reduzirte Form.

Es ist klar, dass eine reduzirte Form als Vertreterin aller ihr äquivalenten Formen gebraucht werden kann.

Ferner leuchtet ein, dass für jede gegebene Determinante die Anzahl aller reduzirten Formen stets eine begränzte ist. Man wird leicht ermessen, wie alle diese reduzirten Formen darzustellen sind. Ist z. B. die Determinante D positiv und kein Quadrat; so braucht man für P_m nach und nach nur alle ganzen Zahlen zu nehmen, welche absolut $\leqq \sqrt{\frac{D}{5}}$ sind. Ist p eine solche; so sind für Q_m und Q_{m-1} alle möglichen Faktorenpaare zu nehmen, in welche sich $D - p^2$ zerlegen lässt.

Von den reduzirten Formen können mehrere unter einander äquivalent sein. Welche der ersteren einander äquivalent sind, lässt sich durch das obige Verfahren entscheiden. Hierdurch zerfällt die Gesammtheit jener reduzirten Formen in Klassen von unter sich äquivalenten Formen. Jede Form einer solchen Klasse ist als ein Repräsentant der ganzen Klasse anzusehen. Die Klassifizirung erleichtert sich durch die sub VII. mitgetheilte Beziehung, wonach man für P_m nur positive Werthe und für Q_m nur Werthe, welche absolut $\leqq Q_{m-1}$ sind, zuzulassen braucht. Bei positiver nicht quadratischer Determinante, wo die beiden äusseren Glieder der reduzirten Form entgegengesetzte Zeichen haben, kann man auch stets dafür sorgen, dass das erste Glied positiv sei, indem dann jedoch nicht nothwendig $Q_m \leqq Q_{m-1}$ werden wird.

Wäre z. B. die Determinante $D = 7$; so hat man, da $\sqrt{\frac{7}{5}}$ zwischen 1 und 2 liegt, für P_m nur die beiden Werthe 0 und 1 zu betrachten. Da nun $7 - 0^2 = 7 = 1 . 7 = 7 . 1$ und $7 - 1^2$

$= 6 = 1 . 6 = 2 . 3 = 6 . 1 = 3 . 2$ ist; so hat man im Ganzen nur die sechs reduzirten Formen $(a, b, c) = (1, 0, 7), (7, 0, 1), (1, 1, 6), (2, 1, 3), (6, 1, 1), (3, 1, 2)$.

Diese sechs Formen gehören jedoch nur zwei Klassen an, indem folgende in Ein und derselben Horizontalreihe stehenden je drei Formen einander äquivalent sind

$$(1, 0, 7),\ (1, 1, 6),\ (2, 1, 3)$$
$$(7, 0, 1),\ (6, 1, 1),\ (3, 1, 2)$$

Die fraglichen beiden Klassen für die Determinante 7 werden also repräsentirt durch die beiden Formen $x^2 - 7y^2$ und $7x^2 - y^2$.

X. Käme es darauf an, für eine gegebene Determinante diejenigen Klassen der reduzirten Formen zu bestimmen, wodurch eine gegebene Zahl q dargestellt werden kann; so hat man unter den positiven Zahlen p, welche $\leqq \frac{q}{2}$ sind, diejenigen zu ermitteln, wodurch $D - p^2$ durch q theilbar wird. Ist p eine solche und $D - p^2 = qr$; so hat man jede der hieraus sich ergebenden Formen (q, p, r) zu reduziren.

Wenn die darzustellende Zahl q eine Primzahl ist, *gibt* es bekanntlich nur einen einzigen Werth für p, also auch nur eine einzige Klasse von reduzirten Formen, wodurch (bei gegebener Determinante) die Zahl q darstellbar wäre.

Sollte z. B. für $D = 7$ die Primzahl $q = 29$ dargestellt werden; so hat man $p = 6$, $7 - 6^2 = -29 = 29(-1)$ und $r = -1$. Die zu reduzirende Form ist also $(29, 6, -1) = 29x^2 - 12xy + y^2$ und man findet, dass dieselbe äquivalent ist der ersteren der oben angeführten beiden Klassen, an deren Spitze die Form $(1, 0, 7) = x^2 - 7y^2$ steht.

XI. Wir machen darauf aufmerksam, dass für die Untersuchungen über quadratische Formen auch die Kettenbruchsentwickelung nach dem Subtraktionsprinzipe, §. 99, eine besondere Wichtigkeit hat, indem nach der dortigen Formel (6) die Kettenbruchsentwickelung von K sofort ohne Zeichenwechsel die äquivalenten Formen ergibt, sodass man bei dieser Entwickelung die Äquivalenz zweier Formen nicht auf doppelte Weise zu prüfen braucht.

Auch liesse sich bei Kettenbrüchen nach dem Additionsprinzipe die Transformation anstatt auf §. 68, Gl. (2), auf die dortige Gl. (12) und bei Kettenbrüchen nach dem Subtraktionsprinzipe auf die der letzteren Gleichung entsprechende Formel basiren.

Zu weiteren Untersuchungen über diesen Gegenstand müssen wir auf die *Disq. arithm.* von Gauss verweisen, woselbst die quadratischen Formen sehr ausführlich, wenngleich nach anderen Prinzipien, als vorstehend, behandelt und zur Auflösung der unbestimmten Gleichungen vom zweiten Grade benutzt sind.

Schliesslich theilen wir auf der folgenden Seite eine kurze Tabelle der verschiedenen reduzirten Formen für die Determinanten von 0 bis 10 und von -1 bis -10 mit.

Es ist dabei zu bemerken, dass für die Determinante null die aus den Koeffizienten aller einander äquivalenten Formen genommenen drei zusammengehörigen Zahlen a, b, c immer Ein und dasselbe grösste gemeinschaftliche Maass w enthalten (§. 93, III). Dieses Maass kann jeden beliebigen Werth besitzen: da aber jedenfalls auch die rechte Seite der quadratischen Form durch w theilbar sein muss; so leuchtet ein, dass man in den meisten Fällen jenes Maass w ausser Acht lassen kann.

Ferner bemerken wir, dass für jede quadratische Determinante d^2 die verschiedenen Klassen nicht äquivalenter Formen ohne alle Rechnung gefunden werden können. Es gibt deren nämlich immer $2d$, welche erhalten werden, indem man in dem Ausdrucke $2dxy + ry^2$ für den Koeffizienten r des zweiten Gliedes entweder die positiven Zahlen von 0 bis $2d - 1$ oder die negativen Zahlen von 0 bis $-(2d-1)$ oder auch die positiven und negativen Zahlen von ± 1 bis $\pm(d-1)$ und ausserdem die Zahl 0 und die Zahl $+d$ oder $-d$ substituirt (durch welche letztere Substitution alle entstehenden Formen den obigen Bedingungen der reduzirten Formen entsprechen würden). Es leuchtet nämlich ein, dass stets zwei Formen wie $2dxy + cy^2$ und $2dxy - (2d - c)y^2$ einander äquivalent sind, indem darin die Differenz der Koeffizienten von y^2 durch $2d$ theilbar ist, also der durch die Eine dargestellte Schluss einer Kettenbruchsentwickelung nach einer paaren Menge von Entwickelungsstufen in den durch die andere dargestellten Schluss transformirt werden kann (§. 89, I.) Dagegen sind zwei Formen wie $2dxy + cy^2$ und $2dxy + c'y^2$, worin c und c' gleiche Zeichen haben und $< 2d$ sind, einander nicht äquivalent, indem nach §. 89 die eben erwähnte Übereinstimmung des Schlusses nur denkbar ist, wenn die Summe von c und c' den numerischen Werth $2d$ hat, in welchem Falle aber die Übereinstimmung nach einer unpaaren Menge von Entwickelungsstufen erfolgt, was von der zweiten Form $2dxy + c'y^2$ wol auf die äquivalente Form $-2dxy - cy^2$ oder $2dxy - cy^2$, nicht aber auf die erste Form $2dxy + cy^2$ führt.

Hinsichtlich der reduzirten Formen mit positiver nicht quadratischer Determinante verdient noch bemerkt zu werden, dass weder der erste, noch der letzte Koeffizient den numerischen Werth der Determinante D übersteigen kann, und dass wenn Einer von beiden dieses Maximum erreicht, der andere numerisch $= 1$ und der mittlere $= 0$ ist. Ausserdem besitzen der erste und letzte Koeffizient immer entgegengesetzte Zeichen.

Eben derselbe Satz gilt für die reduzirten Formen mit negativer Determinante, wobei jedoch die Zeichen des ersten und letzten Koeffizienten einander gleich sind.

Von den reduzirten Formen mit negativer Determinante haben wir nur diejenigen angemerkt, in welchen der erste und letzte Koeffizient positiv ist, welche also nur positive Zahlen darstellen. Nimmt man alle diese Formen mit entgegengesetzten Zeichen; so ergeben sich noch ebenso viel neue nicht äquivalente Formen, welche nur negative Zahlen darstellen.

Dass in jeder reduzirten Form das mittlere in xy multiplizirte Glied nach Belieben positiv oder negativ genommen werden kann, erhellet aus dem obigen Satze VII.

Tafel reduzirter Formen.

Determinante	Reduzirte Formen		Determinante	Reduzirte Formen	Determinante	Reduzirte Formen
0	wx^2 oder wenn man		2	$x^2 - 2y^2$	-1	$x^2 + y^2$
	v. dem gemein-		3	$x^2 - 3y^2$	-2	$x^2 + 2y^2$
	schaftl. Maasse			$3x^2 - y^2$	-3	$x^2 + 3y^2$
	w abstrahirt, . x^2		5	$x^2 - 5y^2$		$2x^2 + 2xy + 2y^2$
	$-wx^2$ „ „ „ „ „ $-x^2$			$2x^2 + 2xy - 2y^2$	-4	$x^2 + 4y^2$
			6	$x^2 - 6y^2$		$2x^2 + 2y^2$
	nach Belieben			$6x^2 - y^2$	-5	$x^2 + 5y^2$
	entweder	oder	7	$x^2 - 7y^2$		$2x^2 + 2xy + 3y^2$
1	$2xy$	$2xy$		$7x^2 - y^2$	-6	$x^2 + 6y^2$
	$2xy + y^2$	$2xy - y^2$	8	$x^2 - 8y^2$		$2x^2 + 3y^2$
4	$4xy$	$4xy$		$2x^2 - 4y^2$	-7	$x^2 + 7y^2$
	$4xy + y^2$	$4xy - 3y^2$		$8x^2 - y^2$		$2x^2 + 2xy + 4y^2$
	$4xy + 2y^2$	$4xy - 2y^2$	10	$x^2 - 10y^2$	-8	$x^2 + 8y^2$
	$4xy + 3y^2$	$4xy - y^2$		$2x^2 - 5y^2$		$2x^2 + 4y^2$
9	$6xy$	$6xy$				$3x^2 + 2xy + 3y^2$
	$6xy + y^2$	$6xy - 5y^2$			-9	$x^2 + 9y^2$
	$6xy + 2y^2$	$6xy - 4y^2$				$3x^2 + 3y^2$
	$6xy + 3y^2$	$6xy - 3y^2$				$2x^2 + 2xy + 5y^2$
	$6xy + 4y^2$	$6xy - 2y^2$			-10	$x^2 + 10y^2$
	$6xy + 5y^2$	$6xy - y^2$				$2x^2 + 5y^2$

Allgemeine Gleichungen des zweiten Grades mit zwei Unbekannten, wenn die Determinante verschieden von null ist.

§. 125. ***Generelle Auflösung dieser Gleichungen in ganzen Zahlen.***

I. Die gegebene Gleichung habe die Form

(1) $$ax^2 - 2bxy - cy^2 + 2dx + 2ey = k.$$

worin also nöthigenfalls durch Multiplikation der ganzen Gleichung mit 2 dafür gesorgt werden muss, dass die Koeffizienten der xy, x, y enthaltenden Glieder paare Zahlen seien.

Wenn x und y ganze Zahlen sind; so werden auch stets die Grössen

(2) $$X = (b^2 + ac)\, x - be + cd$$

(3) $$Y = (b^2 + ac)\, y - ae - bd$$

es sein. Substituirt man die hieraus für x und y sich ergebenden Werthe

(4) $$x = \frac{X + be - cd}{b^2 + ac}$$

(5) $$y = \frac{Y + ae + bd}{b^2 + ac}$$

in die gegebene Gleichung; so nimmt dieselbe folgende Form an, welche wir die reduzirte Gleichung nennen wollen.

(7) $$aX^2 - 2bXY - cY^2 = (b^2 + ac)\,[(b^2 + ac)\,k - (ae^2 + 2bed - cd^2)]$$

Vor allen Dingen bemerken wir, dass die vorstehende Transformation in dem einzigen Falle unstatthaft ist, wo $b^2 + ac = 0$ ist, weil in diesem Falle nach (2) und (3) die Grössen X, Y wie konstante und nach (4) und (5) die Grössen x, y wie unendlich grosse Werthe erscheinen würden. Dieser Fall wird in §. 130 ff. besonders behandelt werden.

Wenn aber die Grösse $b^2 + ac$, welche auch hier die Determinante heisse und mit D bezeichnet werde, verschieden von null ist, nimmt die reduzirte Gleichung (6) genau die Form einer Gleichung an, welche für X und Y nach §. 100 aufgelös't werden kann. Hierbei ist beachtenswerth, dass $D = b^2 + ac$ auch die Determinante der reduzirten Gleichung ist, und dass überhaupt die Grössen X^2, XY, Y^2 der letzteren Gleichung dieselben Koeffizienten besitzen, wie resp. die Grössen x^2, xy, y^2 in der gegebenen Gleichung (1). Die Determinante D erscheint als ein Faktor der rechten Seite der reduzirten Gleichung.

II. Nachdem durch Auflösung der reduzirten Gleichung die Werthe von X, Y gefunden sind, ergeben sich die von x, y, also die Auflösungen der Gl. (1), durch die Formeln (4), (5). Da aber x, y ganze Zahlen sein müssen; so sind nur diejenigen Werthe von X, Y brauchbar, welche, in (4) und (5) substituirt, die Ausdrücke auf den rechten Seiten zu ganzen Zahlen machen.

Die Aufsuchung dieser Werthe von X, Y oder wenn es deren nicht gibt, die Überzeugung von der Unmöglichkeit derselben, ist leicht beschafft, wenn die Determinante D ein Quadrat oder negativ ist, weil alsdann die reduzirte Gleichung nur eine endliche Menge von Auflösungen X, Y zulässt, welche leicht alle geprüft werden können. Anders ist Dies, wenn die

Determinante positiv und nicht quadratisch ist, also eine unendliche Menge von Auflösungen X, Y vorhanden sind.

Diese Auflösungen von X, Y gruppiren sich im letzteren Falle nach §. 100 immer in eine bestimmte Anzahl unendlicher Reihen. Jede dieser Reihen ist für sich zu prüfen. Man erwägt dabei, dass die Ein und derselben Reihe angehörigen Werthe von X, Y die in §. 84 mit $\overset{n}{M}$, $\overset{n}{N}$ bezeichneten Grössen sind, welche aus den zwei zuerst sich ergebenden Paaren $\overset{0}{M}$, $\overset{0}{N}$ und $\overset{1}{M}$, $\overset{1}{N}$ mit Hülfe der Grösse h nach demselben Gesetze entstehen, wie die Zähler und Nenner der Näherungswerthe eines nach dem Subtraktionsprinzipe gebildeten Kettenbruchs. Setzt man nun

(7) $$A = -be + cd$$

(8) $$B = -ae - bd$$

so müssen nach Gl. (4), (5) diejenigen Werthe von M und N ermittelt werden, für welche

(9) $$x = \frac{M - A}{D} \text{ und auch}$$

(10) $$y = \frac{N - B}{D}$$

ganze Zahlen sind.

Hierzu verhilft die Untersuchung in §. 86. Wir können hierbei, da es nur auf die Theilbarkeit von $M - A$ und $N - B$ durch D ankommt, unter D den numerischen Werth der Determinante verstehen. Wenn nun A oder B positiv und $\geqq D$, sowie auch dann, wenn A oder B negativ sind, dividirt man zuvörderst mit D in A, resp. in B, indem man bei dieser Division den grössten Subquotienten nimmt, und bestimmt den Rest der Division, welcher in beiden Fällen positiv und $< D$ sein wird, sodass also, wenn man hierdurch

(11) $$A = wD + A' \text{ und } B = wD + B'$$

erhält, A' und B' positiv und $< D$ sind. Jetzt müssen offenbar auch

$$\frac{M - A'}{D} \text{ und } \frac{N - B'}{D}$$

ganze Zahlen sein, und Dies ist der Fall für alle diejenigen Werthe von M und N, welche in Beziehung zum Divisor D resp. den Rest A' und B' haben, für welche also

(12) $$M \equiv A' \text{ und } N \equiv B'$$

ist.

Demnach bildet man nach §. 86 in Beziehung zum Divisor D erst die Reste der Grössen $\overset{0}{M}$, $\overset{1}{M}$, $\overset{2}{M}$... und dann die Reste

der Grössen $\overset{0}{N}, \overset{1}{N}, \overset{2}{N}\ldots$, welche beide periodisch sein werden, und sucht in derjenigen ersten Periode, welche für die Reste von M und N eine gleiche Länge hat, die Reste von M aus, welche $=A'$ sind, und die Reste von N, welche $=B'$ sind. Gibt es derartige Reste, und besitzen dieselben in den beiden Restreihen von M und N gleiche Zeiger, ist also zugleich

$$(13) \qquad \overset{n}{M} \equiv A' \text{ und } \overset{n}{N} \equiv B'$$

so ist die Auflösung der gegebenen Gleichung in ganzen Zahlen möglich, und zwar hat man, wenn die genannte Periode der Reste von M und N s Glieder besitzt, für jeden in dieser Periode liegenden Zeiger n, für welchen die Beziehungen (13) realisirt sind, eine besondere Reihe Werthe von X und Y. Eine solche Reihe ist dargestellt durch

$$(14) \qquad X = \ldots \overset{n-2s}{M}, \overset{n-s}{M}, \overset{n}{M}, \overset{n+s}{M}, \overset{n+2s}{M}\ldots$$

$$(15) \qquad Y = \ldots \overset{n-2s}{N}, \overset{n-s}{N}, \overset{n}{N}, \overset{n+s}{N}, \overset{n+2s}{N}\ldots$$

Nachdem man durch das Subtraktionsprinzip, welches der Bildung der Grössen M, N aus den beiden ursprünglich berechneten Paaren $\overset{0}{M}, \overset{0}{N}$ und $\overset{1}{M}, \overset{1}{N}$ zu Grunde liegt, zwei benachbarte Paare der vorstehenden Reihen (14), (15), also z. B. die beiden Paare $\overset{n}{M}, \overset{n}{N}$ und $\overset{n+s}{M}, \overset{n+s}{N}$ vermittelst der Grösse k nach §. 84 berechnet hat, ergeben sich alle übrigen in vorwärts und rückwärts schreitender Reihenfolge nach der Methode des §. 85 mit Hülfe der dortigen Grösse H, welche am einfachsten nach der dortigen Gleichung (3) oder auch nach der dortigen Gleichung (6) berechnet werden kann.

Beachtet man, dass in der zu letzterem Zwecke zu verwendenden Gl. (13) in §. 85 die Grösse r, also auch die Grösse rs, stets einen paaren Werth hat, dass mithin immer $(-1)^{rs} = 1$ und $(-1)^{rs-1} = -1$ sein wird; so hat man für die vorwärts, resp. rückwärts liegenden Grössen $M = X$ die Formeln

$$(16) \qquad \overset{n+2s}{M} = H\overset{n+s}{M} - \overset{n}{M}$$

$$(17) \qquad \overset{n-s}{M} = H\overset{n}{M} - \overset{n+s}{M}$$

welche auch, wenn man darin N statt M setzt, für die Grössen $N = Y$ gelten. Man sieht, dass diese Formeln auch hier stets das Subtraktionsprinzip bekunden.

III. Man darf nicht übersehen, dass für X, Y alle Auflösungen der reduzirten Gleichung (6) in relativ primen Zahlen und alle mit gemeinschaftlichem Maasse zu berücksichtigen sind, auch dass jede für X, Y gefundene Auflösung mit entgegengesetzten Zeichen genommen werden kann, ja

dass, wenn $b=0$ sein sollte, das Zeichen von X und das von Y für sich umgekehrt werden kann. Die schliesslich für x und y nach Gl. (4) und (5) sich ergebenden Werthe gestatten eine solche Umkehrung der Zeichen nicht.

Es muss noch darauf aufmerksam gemacht werden, dass die rechte Seite der reduzirten Gl. (6) stets den Faktor $b^2+ac=D$, also die Form DE besitzt. Dies erleichtert nach §. 79 die Aufsuchung der Reihen der durch DE theilbaren Zahlen J von der Form $D-p^2$.

Schliesslich bemerken wir, dass jede nach obiger Methode gefundene Reihe von Auflösungen für x, y von den Mittelgliedern nach beiden Seiten in numerischer Beziehung eine steigende Progression bildet. Da man nun $\frac{x}{y}=\frac{X-A}{Y-B}$ hat; so wird für unendlich grosse Werthe von x und y das Verhältniss $\frac{x}{y}=\frac{X}{Y}=\frac{\pm\sqrt{D}+P_0}{Q_0}$, sodass sich in jeder Reihe das Verhältniss der nach oben und unten immer weiter von der Mitte sich entfernenden Grössen x, y dem Verhältnisse der korrespondirenden Grössen X, Y nähert, welches durch den Doppelwerth der Wurzel der Gleichung $ax^2-2bxy-c=0$ dargestellt ist (s. §. 100, I.)

§. 126. *Beispiel mit positiver nicht quadratischer Determinante:*

$$3x^2-10xy+6y^2+8x-2y=11$$

I. Identifizirt man diese Gleichung mit der im vorhergehenden Paragraphen als gegeben vorausgesetzten Gleichung von der Form

$$ax^2-2bxy-cy^2+2dx+2ey=k$$

so hat man

$$3x^2-2.5xy-(-6)y^2+2.4x+2(-1)y=11$$

also

$$D=\quad b^2+ac=\quad 5^2+3(-6)=7$$
$$A=-be+cd=-5(-1)+(-6)4=-19$$
$$B=-ae-bd=-3(-1)-5.4=-17$$
$$E=\quad(b^2+ac)k-(ae^2+2bed-cd^2)=7.11-[3(-1)^2+2.5(-1)4-(-6)4^2]=18$$
$$DE=\quad 7.18=126$$

Die reduzirte Gleichung ist also

$$3X^2-2.5XY-(-6)Y^2=7.18=126$$

Zur Auflösung dieser Gleichung hat man $K=\frac{\sqrt{7}+5}{3}$ zu entwickeln. Dies gibt

n	P_n	Q_n	a_n	M_n	N_n
-2.				0	1
-1		-6		1	0
0	5	3	2	2	1
1	1	2	1	3	1
2	1	3	1	5	2
3	2	1	4	23	9
4	2	3	1	28	11
5	1	2	1	51	20

Jetzt sind die Reihen der durch 126 theilbaren Zahlen J von der Form $7-p^2$ zu suchen. Es finden sich bei dieser Ermittelung (welche sich durch die Zerlegung der Zahl 126 in die Faktoren $DE=7.18$ nach §. 79 erleichtert) nur zwei Reihen, für welche $p=\pm 49$ ist.

II. Der erste Werth $K'=\frac{\sqrt{7}+49}{126}$ gibt

n	P'_n	Q'_n	a'_n
-1		-19	
0	49	126	0
1	-49	-19	2
2	11	6	2
3	1	1	3
4	2	3	1
5	1	2	1
6	1	3	1
7	2	1	4
8	2	3	1

Die Perioden von K und K' stimmen überein, und zwar bei Gliedern, deren Zeigersumme $m+m'$ eine paare Zahl ist. Demnach liefern die beiden Kombinationen

$K(1)$ *komb.* $K'(5)$

n	a_n	M_n	N_n
-1		1	0
0		2	1
1	0	1	0
2	-1	1	1
3	-3	-2	-3
4	-2	5	7
5	-2	-12	-17

$\overset{0}{M}=-12,\ \overset{0}{N}=-17$

$K(5)$ *komb.* $K'(5)$

n	a_n	M_n	N_n
3		23	9
4		28	11
5	0	23	9
6	-1	5	2
7	-3	8	3
8	-2	-11	-4
9	-2	30	11

$\overset{1}{M}=30,\ \overset{1}{N}=11$

Der Werth von $h=\mathfrak{M}_{r-1}+\mathfrak{N}_{r-2}$ nach §. 82 und 84 findet sich aus der Periode von K, also aus [1, 1, 4, 1], folgendermaassen

n	$\mathfrak{a}_n$	$\mathfrak{M}_n$	$\mathfrak{N}_n$
-2		0	1
-1		1	0
0	1	1	1
1	1	2	1
2	4	9	5
$r-1=3$	1	11	6

Hiernach hat man $h=11+5=16$.

Es ist nun nicht von Interesse, **alle** Werthe von M und N, welche, für X und Y genommen, Auflösungen der reduzirten Gleichung ergeben, zu berechnen, sondern nur diejenigen, welche, eingeführt in die Formeln

$$x = \frac{M - A}{D} = \frac{M - (-19)}{7}$$

$$y = \frac{N - B}{D} = \frac{N - (-17)}{7}$$

für x und y ganze Zahlen liefern. Zu diesem Ende hat man behuf Bestimmung der kleinsten positiven Reste von A und B in Beziehung zum Divisor D

$$A = -19 = -3.7 + 2 \quad \text{also } A' = 2$$

$$B = -17 = -3.7 + 4 \qquad B' = 4$$

Es müssen mithin die Reste von M und N in Beziehung zum Divisor 7 gleichzeitig resp. $= 2$ und 4 sein. Bilden wir nun die Reste der Grössen $\overset{0}{M}$, $\overset{1}{M}$, $\overset{2}{M}\ldots$ und der Grössen $\overset{0}{N}$, $\overset{1}{N}$, $\overset{2}{N}\ldots$ nach §. 86, indem wir zur Ökonomie der Rechnung beachten, dass

$$h = 16 = 2.7 + 2 \equiv 2, \text{ ferner}$$

$$\overset{0}{M} = -12 = -2.7 + 2 \equiv 2 \qquad \overset{0}{N} = -17 = -3.7 + 4 \equiv 4$$

$$\overset{1}{M} = 30 = 4.7 + 2 \equiv 2 \qquad \overset{1}{N} = 11 = 1.7 + 4 \equiv 4$$

ist, und dass bei der Bildung der Grössen M und N stets das **Subtraktionsprinzip** zur Anwendung kommt; so ergibt sich als erste Periode dieser Reste:

n	Rest von h	Rest von $\overset{n}{M}$
0	2	2
1	2	2
2	2	6
3	2	0
4	2	6
5	2	5
6	2	2
7	2	2

n	Rest von h	Rest von $\overset{n}{N}$
0	2	4
1	2	4
2	2	5
3	2	0
4	2	5
5	2	3
6	2	4
7	2	4

In dieser Periode, für welche $s = 6$ ist, entsprechen der obigen Bedingung zuvörderst die Grössen $\overset{0}{M}$, $\overset{0}{N}$ für den Zeiger $n = 0$, alsdann aber auch die Grössen $\overset{1}{M}$, $\overset{1}{N}$ für den Zeiger $n = 1$; sonst keine. Die gesuchten Werthe von M und N sind also in folgenden beiden Reihen darzustellen

$$X = \ldots \overset{-12}{M}\ \overset{-6}{M}\ \overset{0}{M}\ \overset{6}{M}\ \overset{12}{M} \ldots$$

$$Y = \ldots N\ N\ N\ N\ N \ldots$$

und

$$X = \ldots \overset{-11}{M}\,\overset{-5}{M}\,\overset{1}{M}\,\overset{7}{M}\,\overset{13}{M}\ldots$$
$$Y = \ldots N\; N\; N\; N\; N \ldots$$

Um die Werthe einer jeden Reihe nach den Rekursionsformeln des §. 85 zu berechnen, ist zuvörderst die Grösse H zu bestimmen. Die dortige Formel (3) gibt hierfür, da $h = 16$ und $s = 6$ ist,

$$H = 16^6 - 6.16^4 + \frac{6.3}{1.2}.16^2 - \frac{6.2.1}{1.2.3}.16^0 = 16386302$$

Jetzt muss, um zuvörderst die in der ersten obigen Reihe enthaltenen Werthe von M und N zu berechnen, ausser dem bereits bekannten Paare $\overset{0}{M} = -12$, $\overset{0}{N} = -17$ noch das benachbarte $\overset{6}{M}$, $\overset{6}{N}$ bestimmt werden. Dies kann unter Zuhülfenahme der Werthe $\overset{1}{M} = 30$, $\overset{1}{N} = 11$ und der Grösse $h = 16$ durch die Rekursionsmethode des §. 84 geschehen. Es wird jedoch einfacher und für die späteren Rechnungen vortheilhaft sein, hierzu die Formel (9) aus §. 85 zu nehmen. Dieselbe ist hier, wo das Subtraktionsprinzip gilt,

$$\overset{n}{M} = h_{n-1}\overset{1}{M} - h_{n-2}\overset{0}{M}$$

Um dieselbe zu benutzen, sind zuvor die Grössen h_n, welche auch späterhin noch mehrfach gebraucht werden, zu bilden. Für die letzteren Grössen hat man, wenn man unter Beachtung des Subtraktionsprinzips das Rekursionsverfahren aus §. 85 in Anwendung bringt,

n	h	h_n
-1	16	0
0	16	1
1	16	16
2	16	255
3	16	4064
4	16	64769
5	16	1032240
6	16	16451071

Jetzt ist nach der soeben zitirten Formel

$$\overset{6}{M} = h_5\overset{1}{M} - h_4\overset{0}{M} = 1032240.30 - 64769(-12) = 31744428$$
$$\overset{6}{N} = h_5\overset{1}{N} - h_4\overset{0}{N} = 1032240.11 - 64769(-17) = 12455713$$

Diese Werthe von $\overset{6}{M}$, $\overset{6}{N}$, in Verbindung mit denen von $\overset{0}{M}$, $\overset{0}{N}$ und dem Werthe von H, liefern nach §. 85 unter Beachtung des Subtraktionsprinzips folgende zulässige Werthe von X und Y

n	H	$\overset{n}{M} = X$	$\overset{n}{N} = Y$
.	.	.	.
.	.	.	.
.	.	.	.
-6	16386302	-228380052	-291022847
0	16386302	-12	-17
6	16386302	31744428	12455713
12	16386302	520173784025268	204103074843343
.	.	.	.
.	.	.	.
.	.	.	.

Jedes Paar dieser Werthe von X, Y führt zu einer Auflösung der ursprünglichen Gleichung nach den Formeln

$$x = \frac{X + 19}{7}, \quad y = \frac{Y + 17}{7}$$

Man hat also zunächst folgende Reihe von Auflösungen

x	y
.	.
.	.
.	.
-32625719	-41574690
1	0
4534921	1779390
74310540575041	29157582120480
.	.
.	.
.	.

Was die zweite Reihe der obigen Werthe von X, Y betrifft; so ist neben dem schon bekannten Paare $\overset{1}{M} = 30$, $\overset{1}{N} = 11$ das Paar $\overset{7}{M}$, $\overset{7}{N}$ zu berechnen. Hierfür hat man nach der schon vorhin gebrauchten Formel

$$\overset{7}{M} = h_6 \overset{1}{M} - h_5 \overset{0}{M} = 16451071 . 30 - 1032240 (-12) = 505919010$$

$$\overset{7}{N} = h_6 \overset{1}{N} - h_5 \overset{0}{N} = 16451071 . 11 - 1032240 (-17) = 198509861$$

Dies gibt folgende Reihen von Werthen für X, Y

n	H	$\overset{n}{M} = X$	$\overset{n}{N} = Y$
.	.	.	.
.	.	.	.
.	.	.	.
-5	16386302	-14329950	-18260539
1	16386302	30	11
7	16386302	505919010	198509861
.	.	.	.
.	.	.	.
.	.	.	.

Substituirt man diese Werthe in die obigen Formeln für x und y; so erzeugt sich die nachstehende Reihe von Auflösungen der gegebenen Gleichung

x	y
.	.
.	.
.	.
-2047133	-2608646
7	4
72274147	28358554
.	.
.	.
.	.

Ehe wir zu den Kombinationen von K mit den übrigen Werthen von K' übergehen, wollen wir diejenigen Auflösungen für x, y untersuchen, welche sich ergeben, wenn man die vorstehend für X, Y gefundenen Werthe mit entgegengesetzten Zeichen nimmt.

Statt dass man die Zeichen aller obigen Werthe von X, Y umkehrt, kann man offenbar die Zeichen von zwei benachbarten Paaren umkehren, und hieraus die übrigen mit Hülfe der Grösse $h = 16$ nach dem bekannten Bildungsgesetze, welchem immer das Subtraktionsprinzip zu Grunde liegt, erzeugen. Hiernach hat man zur Darstellung der kleinsten Reste in Beziehung zu dem Divisor $D = 7$

$h = 16 = 2.7 + 2 \equiv 2$, ferner

$\overset{0}{M} = 12 = 1.7 + 5 \equiv 5$ $\quad \overset{0}{N} = 17 = 2.7 + 3 \equiv 3$

$\overset{1}{M} = -30 = -5.7 + 5 \equiv 5$ $\quad \overset{1}{N} = -11 = -2.7 + 3 \equiv 3$

n	Rest von h	Rest von $\overset{n}{M}$	n	Rest von h	Rest von $\overset{n}{M}$
0	2	5	0	2	3
1	2	5	1	2	3
2	2	5	2	2	3

Man erkennt, dass die Periode dieser Reste eingliederig ist, und dass, da der Rest von M nicht $= 2$ und der von N nicht $= 4$ ist, unter den neuen Werthen von X, Y keine solche vorkommen, welche für x, y ganze Zahlen liefern.

III. Wir schreiten nun zu der Entwickelung des zweiten Werthes von K', welcher $= \frac{\sqrt{7} - 49}{126}$ ist und sich sehr wohl als brauchbar erweisen kann, da der erste schon als zulässig erkannte Werth von K' für $p = +49$ eine symmetrische eingliedrige (beim Zeiger 4 beginnende) Periode besitzt.

Dieser neue Werth von K' gibt

n	P'_n	Q'_n	a'_n
-1		-19	
0	-49	126	-1
1	-77	-47	1
2	30	19	1
3	-11	-6	1
4	5	3	2
5	1	2	1
6	1	3	1
7	2	1	4
8	2	3	1

Die Periode von K' stimmt wiederum mit der von K so überein, dass die Zeigersumme $m+m'$ eine paare Zahl ist.

Demnach hat man die beiden Kombinationen

$K(1)$ *komb.* $K'(5)$

n	a_n	M_n	N_n
-1		1	0
0		2	1
1	0	1	0
2	-2	0	1
3	-1	1	-1
4	-1	-1	2
5	-1	2	-3

$\overset{0}{M}=2,\ \overset{0}{N}=-3$

$K(5)$ *komb.* $K'(5)$

n	a_n	M_n	N_n
3		23	9
4		28	11
5	0	23	9
6	-2	-18	-7
7	-1	41	16
8	-1	-59	-23
9	-1	100	39

$\overset{1}{M}=100,\ \overset{1}{N}=39$

Die Grösse h behält hier und durch den ganzen Verlauf der Auflösung der gegebenen Gleichung denselben Werth 16; ebenso bleibt stets $D=7$. Um also die Reste der Grössen M und N zu bilden, hat man

$h=16=2.7+2\equiv 2$, ferner

$\overset{0}{M}=2 \qquad \overset{0}{N}=-\ 3=-1.7+4\equiv 4$

$\overset{1}{M}=100=14.7+2\equiv 2 \qquad \overset{1}{N}=\ 39=\ 5.7+4\equiv 4$

Da die Reste der ersten beiden Werthe von M, sowie die der ersten beiden Werthe von N resp. $=2$ und 4, wie früher sind; so leuchtet ein, dass auch alle folgenden Reste mit den früheren übereinstimmen werden. Demnach gibt es auch hier zwei besondere Reihen zulässiger Werthe von $X=\overset{n}{M}$ und $Y=\overset{n}{N}$, welchen, da auch hier die Periode der Reste $s=6$ Glieder hat, resp. die Zeigerreihen

$$\ldots -12,\ -6,\ 0,\ 6,\ 12\ldots \text{ und}$$
$$\ldots -11,\ -5,\ 1,\ 7,\ 13\ldots$$

zukommen.

Für die erste Reihe ist

$$\overset{6}{M}=h_5\overset{1}{M}-h_4\overset{0}{M}=1032240.100-64769\ .2\ =103094462$$
$$\overset{6}{N}=h_5\overset{1}{N}-h_4\overset{0}{N}=1032240.\ 39-64769(-3)=\ 40451667$$

Diese Werthe von $\overset{6}{M}$, $\overset{6}{N}$, in Verbindung mit den Werthen

von $\overset{0}{M}$, $\overset{0}{N}$ und der Grösse H, welche hier wegen $s=6$ den obigen Werth 16386302 besitzt, liefern folgende Reihe zulässiger Werthe von X, Y, wovon wir nur die zwei so eben schon gefundenen notiren wollen:

n	H	$\overset{n}{M}=X$	$\overset{n}{N}=Y$
.	.	.	.
.	.	.	.
.	.	.	.
0	16386302	2	-3
6	16386302	103094462	40451667
.	.	.	.
.	.	.	.
.	.	.	.

Eine Substitution dieser Werthe von X, Y in die obigen Formeln für x, y ergibt folgende Auflösungen der gegebenen Gleichung:

x	y
.	.
.	.
.	.
3	2
147277783	57778812
.	.
.	.
.	.

Für die zweite Reihe ist

$$\overset{7}{M}=h_6\overset{1}{M}-h_5\overset{0}{M}=16451071.100-1032240\ .2\ =1643042620$$
$$\overset{7}{N}=h_6\overset{1}{N}-h_5\overset{0}{N}=16451071.\ 39-1032240(-3)=\ 644688489$$

Diese Werthe von $\overset{7}{M}$, $\overset{7}{N}$, in Verbindung mit denen von $\overset{1}{M}$, $\overset{1}{N}$, liefern für X, Y

n	H	$\overset{n}{M}=X$	$\overset{n}{N}=Y$
.	.	.	.
.	.	.	.
.	.	.	.
1	16386302	100	39
7	16386302	1643042620	644688489
.	.	.	.
.	.	.	.
.	.	.	.

und demnach für x, y

x	y
.	.
.	.
.	.
17	8
234720377	92098358
.	.
.	.
.	.

Nimmt man jetzt die Werthe von X, Y aus den letzteren beiden Reihen mit entgegengesetzten Zeichen; so werden dieselben genau so wie die früher mit entgegengesetzten Zeichen genommenen Grössen dieser Art resp. nur den Rest 5 und den Rest 3 ergeben, also sämmtlich unzulässig sein.

IV. Jetzt ist noch zu berücksichtigen, dass die rechte Seite der reduzirten Gleichung einen quadratischen Faktor besitzt, indem man $126 = 3^2 . 14$ hat. Demnach sind die Auflösungen X, Y zu untersuchen, welche das gemeinschaftliche Maass 3 besitzen, für welche man also

$$X = 3X' \qquad Y = 3Y'$$
$$3X'^2 - 2.5X'Y' - (-6)Y'^2 = 14$$

hat. Die Grösse K behält immer den nämlichen Werth $\frac{\sqrt{7}+5}{3}$. Was die Grösse K' betrifft; so gibt es nur eine einzige, nämlich symmetrische Reihe der durch 14 theilbaren Zahlen von der Form $7 - p^2$. Dieser Reihe entspricht der Werth $p = 7$. Man hat also für $K' = \frac{\sqrt{7}+7}{14}$,

n	P'_n	Q'_n	a'_n
-1		-3	
0	7	14	0
1	-7	-3	1
2	4	3	2
3	2	1	4
4	2	3	1
5	1	2	1
6	1	3	1
7	2	1	4
8	2	3	1

Diese Periode von K' ist mit der von K so in Übereinstimmung, dass die Zeigersumme $m + m'$ eine paare Zahl bildet. Demnach hat man die beiden Kombinationen

$K(1)$ *komb.* $K'(5)$

n	a_n	M_n	N_n
-1		1	0
0		2	1
1	0	1	0
2	-1	1	1
3	-4	-3	-4
4	-2	7	9
5	-1	-10	-13

$X' = -10, \quad Y' = -13$

$\overset{0}{M} = X = 3X' = -30, \quad \overset{0}{N} = Y = 3Y' = -39$

$K(5)$ *komb.* $K'(5)$

n	a_n	M_n	N_n
3		23	9
4		28	11
5	0	23	9
6	-1	5	2
7	-4	3	1
8	-2	-1	0
9	-1	4	1

$X' = 4, \quad Y' = 1$

$\overset{1}{M} = X = 3X' = 12, \quad \overset{1}{N} = Y = 3Y' = 3$

Zur Bildung der Reste der Grössen M, N hat man

$h = 16 = 2.7 + 2 \equiv 2$, ferner

$\overset{0}{M} = -30 = -5.7 + 5 \equiv 5 \qquad \overset{0}{N} = -39 = -6.7 + 3 \equiv 3$

$\overset{1}{M} = 12 = 1.7 + 5 \equiv 5 \qquad \overset{1}{N} = .3$

Diese Reste führen zu einer auch oben schon vorgekommenen eingliedrigen Periode, und man erkennt daraus, dass die zugehörigen Grössen X, Y keine brauchbaren Werthe liefern.

Endlich sind noch die vorstehenden Werthe von M, N mit entgegengesetzten Zeichen zu nehmen. Dies gibt

$\overset{0}{M} = 30 = 4.7 + 2 \equiv 2 \qquad \overset{0}{N} = 39 = 5.7 + 4 \equiv 4$

$\overset{1}{M} = -12 = -2.7 + 2 \equiv 2 \qquad \overset{0}{N} = -3 = -1.7 + 4 \equiv 4$

Die Reste sind ebenfalls weiter oben schon vorgekommen. Sie führen zu einer sechsgliedrigen Periode und zu zwei Reihen zulässiger Werthe von M und N, welchen die oben angeführten beiden Zeigerreihen entsprechen.

Um die erste Reihe zu berechnen, hat man

$$\overset{6}{M} = h_5 \overset{1}{M} - h_4 \overset{0}{M} = 1032240\,(-12) - 64769.30 = -14329950$$

$$\overset{6}{N} = h_5 \overset{1}{N} - h_4 \overset{0}{N} = 1032240\,(-\ 3) - 64769.39 = -5622711$$

und da hier wegen der sechsgliedrigen Periode H seinen früheren Werth behält,

n	H	$\overset{n}{M} = X$	$\overset{n}{N} = Y$
.	.	.	.
.	.	.	.
.	.	.	.
0	16386302	30	39
6	16386302	-14329950	-5622711
.	.	.	.
.	.	.	.
.	.	.	.

Dies gibt folgende Auflösungen der gegebenen Gleichung

x	y
.	.
.	.
.	.
7	8
-2047133	-803242
.	.
.	.
.	.

Um die zweite der in Rede stehenden beiden Reihen zu berechnen, hat man

$$\overset{7}{M} = h_6 \overset{1}{M} - h_5 \overset{0}{M} = 16451071\,(-12) - 1032240.30 = -228380052$$

$$\overset{7}{N} = h_6 \overset{1}{N} - h_5 \overset{0}{N} = 16451071\,(-\ 3) - 1032240.39 = -89610573$$

n	H'	$\overset{n}{M}=X$	$\overset{n}{N}=Y$
.	.	.	.
.	.	.	.
.	.	.	.
1	16386302	-12	-3
7	16386302	-228380052	-89610573
.	.	.	.
.	.	.	.
.	.	.	.

Dies gibt folgende Auflösungen für x, y

x	y
.	.
.	.
.	.
1	2
-32625719	-12801508
.	.
.	.
.	.

V. Im Vorstehenden sind 6 verschiedene Reihen von Auflösungen für x, y ermittelt. Ausser den in diesen Reihen liegenden hat die gegebene Gleichung keine Auflösungen. Die in den obigen Reihen vorkommenden Auflösungen in kleinen Zahlen sind

$$x = 1 \quad 1 \quad 3 \quad 7 \quad 7 \quad 17$$
$$y = 0 \quad 2 \quad 2 \quad 4 \quad 8 \quad 8$$

Die Werthe der nächst grösseren Auflösungen liegen schon in den Millionen. An diesem Umstande erkennt man die Nützlichkeit einer direkten und systematischen Methode behuf Auflösung von Gleichungen der gegebenen Art.

§. 127. *Independente Formeln für die Auflösungen der vorstehenden Gleichungen mit positiver nicht quadratischer Determinante.*

Die Auflösungen x, y der gegebenen Gleichung gruppiren sich ebenso wie die Auflösungen X, Y der reduzirten Gleichung in gewisse Reihen. Alle denselben Reihen (14,) (15) in §. 125 angehörigen Werthe $X = \overset{n+ms}{M}$, $Y = \overset{n+ms}{N}$ berechnen sich aus zwei benachbarten Paaren $\overset{n}{M}$, $\overset{n}{N}$ und $\overset{n+s}{M}$, $\overset{n+s}{N}$ mit Hülfe der Grösse H nach dem Subtraktionsprinzipe ebenso wie die Grössen $\overset{n}{M}$, $\overset{n}{N}$ aus den zwei benachbarten Paaren $\overset{0}{M}$, $\overset{0}{N}$ und $\overset{1}{M}$, $\overset{1}{N}$ mit Hülfe der Grösse h. Bezeichnet man also mit H_m eine nach Gl. (2) in §. 85 aus H gebildete Grösse, sodass also

(1) $$H_m = H^m - \overset{m-1}{B_1} h^{m-2} + \overset{m-2}{B_2} h^{m-4} - \overset{m-3}{B_3} h^{m-6} + \text{etc.}$$

ist; so hat man nach demselben Prinzipe, auf welchem die Gl. (9) in §. 85 beruhet, insofern m positiv ist,

(2) $$X = \overset{n+ms}{M} = H_{m-1}\overset{n+s}{M} - H_{m-2}\overset{n}{M}$$

(3) $$Y = \overset{n+ms}{N} = H_{m-1}\overset{n+s}{N} - H_{m-2}\overset{n}{N}$$

Für die rückwärts in der fraglichen Reihe liegenden Werthe von X, Y hat man

(4) $$X = \overset{n-ms}{M} = H_m\overset{n}{M} - H_{m-1}\overset{n+s}{M}$$

(5) $$Y = \overset{n-ms}{N} = H_m\overset{n}{N} - H_{m-1}\overset{n+s}{M}$$

Da nach der Voraussetzung die beiden Paare $\overset{n}{M}$, $\overset{n}{N}$ und $\overset{n+s}{M}$, $\overset{n+s}{N}$ solche Werthe von X, Y sind, welche für x, y ganze Zahlen liefern, und s die Gliederzahl der Periode der Reste der Grössen M, N bezeichnet; so führt jedes durch (2) oder (3) dargestellte Paar von X, Y zu einer Auflösung von x, y; man hat also nach Gl. (9), (10) in §. 125 als independente Formeln für die vorwärts liegenden Werthe von x, y

(6) $$x = \frac{1}{D}(H_{m-1}\overset{n+s}{M} - H_{m-2}\overset{n}{M} - A)$$

(7) $$y = \frac{1}{D}(H_{m-1}\overset{n+s}{N} - H_{m-2}\overset{n}{N} - B)$$

und für die rückwärts liegenden

(8) $$x = \frac{1}{D}(H_m\overset{n}{M} - H_{m-1}\overset{n+s}{M} - A)$$

(9) $$y = \frac{1}{D}(H_m\overset{n}{N} - H_{m-1}\overset{n+s}{N} - B)$$

§. 128. *Besondere Behandlung des Falles, wo die Determinante ein Quadrat, verschieden von null, ist.*

In diesem Falle kann man die reduzirte Gleichung, wenn man es für bequemer hält, auch nach §. 121 auflösen. Dieser Fall ereignet sich unfehlbar dann, wenn das Quadrat von x^2 oder das von y^2 oder von Beiden fehlt, aber das Glied in xy vorhanden ist. Für die wichtigsten Spezialitäten wollen wir im Nachfolgenden einige Beispiele und Bemerkungen mittheilen.

I. **Es fehle das Glied in y^2.** Ein Beispiel dieser Art ist

$$7x^2 - 2xy + 6x - 4y = 1$$

Die reduzirte Gleichung wird

$$7X^2 - 2XY = -15$$

und man hat $D = 1$

$$x = X - 2 \qquad\qquad y = Y - 11$$

Wegen des Werthes $D = 1$ wird also jeder ganze Werth von X und Y auch einen ganzen Werth resp. von x und y liefern.

Für die Auflösung der vorstehenden reduzirten Gleichung sind in §. 121, III. zwei verschiedene Methoden angegeben. Verfährt man nach der zweiten, welche die einfachere ist; so hat man $k = -15$

$p=$	1	3	5	15	-1	-3	-5	-15
$q=$	-15	-5	-3	-1	15	5	3	1

Nun ist $X = p$, $Y = \frac{q - ap}{b} = \frac{q - 7p}{-2}$. Es zeigt sich, dass jede zwei zusammengehörige Werthe von p, q eine ganze Zahl für Y liefern. Man hat also

$X=$	1	3	5	15	-1	-3	-5	-15
$Y=$	11	13	19	53	-11	-13	-19	-53
$x=$	-1	1	3	13	-3	-5	-7	-17
$y=$	0	2	8	42	-22	-24	-30	-64

II. Es fehlen die Glieder in x^2 und y^2. — Ein Beispiel dieser Art ist

$$3xy - 11x + 2y = 18$$

In dieser Gleichung ist die Bedingung nicht erfüllt, dass die Koeffizienten von xy, x, y paare Zahlen seien. Multiplizirt man also zuvor mit 2; so kommt

$$6xy - 22x + 4y = 36$$

Die reduzirte Gleichung ist

$$6XY = 9 . 192 = 1728$$

und hierin hat man $D = 9$, $x = \frac{X - 6}{9}$, $y = \frac{Y + 33}{9}$

Um dieselbe nach §. 121, IV. aufzulösen, kann man zuvor mit 6 dividiren. Dies gibt

$$XY = 288$$

X und Y sind also irgend zwei Faktoren, in welche man die Zahl 288 zerlegen kann. Aus den Formeln $x = \frac{X - 6}{9} = \frac{\frac{1}{3}X - 2}{3}$ und $y = \frac{Y + 33}{9} = \frac{\frac{1}{3}Y + 11}{3}$ erkennt man zur Vereinfachung der Rechnung, dass nur solche Werthe von X und Y brauchbar sind, welche sich durch 3 theilen lassen. Dies sind nur folgende

$X=$	3	6	12	24	48	96	-3	-6	-12	-24	-48	-96
$Y=$	96	48	24	12	6	3	-96	-48	-24	-12	-6,	-3

Damit aber auch x und y ganze Zahlen werden, kann man nur folgende beibehalten

$X=$	6	24	96	-3	-12	-48
$Y=$	48	12	3	-96	-24	-6
$x=$	0	2	10	-1	-2	-6
$y=$	9	5	4	-7	1	3

Allgemein hat man in dem vorstehenden Falle nach 125, Gl. (4), (5) immer, da $a=0$, $c=0$ ist,

$$x=\frac{X+be}{b^2} \qquad y=\frac{Y+bd}{b^2}$$

Wenn man diese Formeln in die Form

$$x=\frac{\left(\frac{1}{b}X\right)+e}{b} \qquad y=\frac{\left(\frac{1}{b}Y\right)+d}{b}$$

bringt, so erkennt man, dass nur solche Werthe von X und Y brauchbar sind, welche sich durch b theilen lassen. Die reduzirte Gleichung ist nach §. 125, Gl. (6)

$$-2bXY=b^3(bk-2ed)$$

oder wenn man mit $-2b^3$ dividirt,

$$\left(\frac{1}{b}X\right)\left(\frac{1}{b}Y\right)=-b.\frac{k}{2}+ed$$

Die in die Ausdrücke für x, y zu substituirenden Grössen $\frac{1}{b}X$, $\frac{1}{b}Y$ sind also zwei Faktoren, in welche sich die Grösse $-b\frac{k}{2}+ed$ zerlegen lässt.

Wenn man nach den letzteren Formeln rechnen will, ist es gleichgültig, ob die Koeffizienten der Glieder in xy, x, y paare Zahlen sind oder nicht. Man kann ohne Weiteres die Koeffizienten von xy, x, y und das konstante Glied rechts resp. für die in den letzteren Formeln vorkommenden Grössen $-b$, d, e, $\frac{k}{2}$ nehmen.

In dem vorstehenden Beispiele

$$3xy-11x+2y=18$$

würde man nach den letzteren Formeln

$$\left(\frac{1}{-3}X\right)\left(\frac{1}{-3}Y\right)=32$$

$$x=\frac{\left(\frac{1}{-3}X\right)+2}{-3} \qquad y=\frac{\left(\frac{1}{-3}Y\right)-11}{-3}$$

haben, was zu den schon vorhin bezeichneten Auflösungen führt.

III. Es fehlen die Glieder in x^2 und y^2 und das in y. — Die Gleichung hat alsdann die einfache Gestalt

$$bxy+dx=k$$

worin es gleichgültig ist, ob die Koeffizienten paar sind oder nicht. Sind p, q zwei Faktoren, in welche sich k zerlegen lässt; so kann man schreiben

$$x(by+d)=pq$$

$$x=p \qquad y=\frac{q-d}{b}$$

Beispiel: $3xy-7x=25$. Hier hat man

$$\begin{array}{lrrrrrr} p= & 1 & 5 & 25 & -1 & -5 & -25 \\ q= & 25 & 5 & 1 & -25 & -5 & -1 \end{array}$$

$$x=p \qquad y=\frac{q+7}{3}$$

Es sind also, damit y eine ganze Zahl werde, folgende Werthe von p, q zulässig

$$\begin{array}{lrrr} p= & 5 & -1 & -25 \\ q= & 5 & -25 & -1 \\ x= & 5 & -1 & -25 \\ y= & 4 & -6 & 2 \end{array}$$

§. 129. ***Besondere Behandlung des Falles, wo die Determinante negativ ist.***

Auch in diesem Falle kann man sich behuf Auflösung der reduzirten Gleichung der besonderen Methode des §. 122 bedienen, insofern man dieselbe für einfacher hält. Als Beispiel diene die Gleichung

$$3x^2+y^2-4x=0$$

Die reduzirte Gleichung ist

$$3X^2+Y^2=12$$

und man hat für die negative Determinante $-D=-3$, ferner

$$x=\frac{X-2}{-3} \qquad y=\frac{Y}{-3}$$

Lös't man die reduzirte Gleichung nach §. 122 auf; so hat man statt der dortigen Gl. (7)

$$36-3Y^2=Z^2$$

Substituirt man hierin für y alle ganzen Zahlen, welche $\leqq\sqrt{\frac{3.12}{3}}$ d. i. $\leqq 3$ sind; so kommt

$$\begin{array}{l} 36-3.0^2=36=6^2 \\ 36-3.1^2=33 \\ 36-3.2^2=24 \\ 36-3.3^2=\ \ 9=3^2 \end{array}$$

Man hat also $\quad Y=\ \ 0,\ \pm 3$

$$Z=\pm 6,\ \pm 3$$

Nach §. 122, Gl. (6) muss aber $X=\frac{Z}{3}$ eine ganze Zahl sein. Dies ereignet sich für jeden vorstehenden Werth von Z; man hat also $\quad X=\pm 2,\ \pm 1$

Berücksichtigt man nun, dass $x=\frac{X-2}{-3}$ und $y=\frac{Y}{-3}$

ganze Zahlen sein müssen; so erhält man folgende Auflösungen

$X=2$	-1	-1
$Y=0$	3	-3
$x=0$	1	1
$y=0$	-1	1

Allgemeine Gleichungen des zweiten Grades mit zwei Unbekannten, wenn die Determinante gleich null ist.

§. 130. ***Auflösung der einfachsten Fälle mit der Determinante null.***

I. $$x^2+y=k$$

In dieser Gleichung kann man für x jeden beliebigen positiven oder negativen ganzen Werth w nehmen; y ist alsdann $=k-x^2$. Man hat also unendlich viel Auflösungen von der Form

(1) $$x=w$$
(2) $$y=k-w^2$$

Wäre die gegebene Gleichung

II. $$ax^2+y=k$$

so hat man auch hier

(3) $$x=w$$
(4) $$y=k-aw^2$$

Wäre gegeben

III. $$x^2+ey=k$$

so sind, da nun $y=\frac{k-x^2}{e}$ ist, für x ganze Werthe von der Beschaffenheit zu nehmen dass $\frac{k-x^2}{e}$ eine ganze Zahl y wird. Zu diesem Ende ermittelt man nach §. 76 oder 77 die durch e theilbaren Zahlen J von der Form $k-x^2$. Dieselben ergeben sich, wenn die Aufgabe möglich ist, reihenweis, und für jede besondere Reihe erhält man einen Werth von x, welcher absolut $\leqq\frac{e}{2}$ ist, und mit u bezeichnet werden möge. Je zwei dieser Reihen, wenn sie nicht kongruent, also symmetrisch sind, entsprechen den beiden Werthen $\pm u$. Diese beiden Werthe wollen wir einfach durch u darstellen, indem wir diese Grösse als **zweideutig** voraussetzen. Der dem Werthe $x=u$ entsprechende Werth von y sei $y=\frac{k-u^2}{e}=v$. Für jedes andere Glied einer solchen Reihe von x hat man nun nach §. 75

(5) $$x=u+ew$$
(6) $$y=v+2uw-ew^2$$

und diese Formeln bilden die generelle Auflösung der gegebe-

nen Gleichung III. Die beiden Grössen u und v besitzen hierin eine endliche Menge zusammengehöriger Werthe. Die Grösse w dagegen ist stets eine willkürliche positive oder negative ganze Zahl.

Beispiel: $$x^2 + 8y = 17$$

Es gibt hier vier Reihen der durch $e = 8$ theilbaren Zahlen J von der Form $17 - x^2$. Dieselben entsprechen den Werthen

$$u = \quad \pm 1 \quad \pm 3$$
$$v = \frac{17 - u^2}{8} = 2 \quad 1$$

Man hat also folgende vier Reihen von Auflösungen

$$\begin{cases} x = \pm 1 + 8w \\ y = 2 \mp 2w - 8w^2 \end{cases}$$
$$\begin{cases} x = \pm 3 + 8w \\ y = 1 \mp 6w - 8w^2 \end{cases}$$

worin die oberen oder die unteren Zeichen zu nehmen sind.

Einige spezielle Werthe der hierdurch dargestellten Auflösungen sind resp. aus der 1sten, 2ten, 3ten, 4ten Reihe

	für $w =$	-2	-1	0	1	2
1ste Reihe	$x =$	-15	-7	1	9	17
	$y =$	-26	-4	2	-8	-34
2te Reihe	$x =$	-17	-9	-1	7	15
	$y =$	-34	-8	2	-4	-26
3te Reihe	$x =$	-13	-5	3	11	19
	$y =$	-19	-1	1	-13	-43
4te Reihe	$x =$	-19	-11	-3	5	13
	$y =$	-43	-13	1	-1	-19

Wäre die Gleichung

IV. $$ax^2 + ey = k$$

gegeben; so erhält man durch Multiplikation mit a

$$(ax)^2 + aey = ak$$

und wenn man

(7) $$X = ax \text{ also } x = \frac{X}{a}$$

setzt,

(8) $$X^2 + aey = ak \text{ also } y = \frac{ak - X^2}{ae}$$

Die letztere vertritt die Stelle der reduzirten Gleichung. Dieselbe kann wie die obige Gl. III. behandelt werden. Man sucht also die durch ae theilbaren Zahlen J von der Form $ak - X^2$. Den einzelnen Reihen dieser Zahlen mögen die Werthe

$$X = U \text{ und } y = \frac{ak - U^2}{ae} = v$$

entsprechen. Es ist aber jetzt zu erwägen, dass nach der Be-

dingung (7) alle Werthe von X durch a theilbar sein müssen. Da nun der allgemeine Ausdruck der Werthe von X die Form $U+aew$ hat, und das zweite Glied dieses Ausdruckes durch a theilbar ist; so muss es auch das erste Glied U sein. Es können also nur diejenigen Werthe von U beibehalten werden, welche sich durch a theilen lassen. Setzt man für dieselben $\frac{U}{a}=u$; so hat man als Auflösung der gegebenen Gleichung

(9) $$x=u+ew$$

(10) $$y=v-2auw-aew^2$$

Beispiel: $$2x^2-3y=23$$

Die reduzirte Gleichung ist hier

$$X^2-6y=46$$

Es gibt zwei Reihen der durch -6 oder 6 theilbaren Zahlen J von der Form $46-X^2$. Dieselben entsprechen den Werthen $U=\pm 8$, und man hat dafür $v=\frac{46-8^2}{-6}=3$. Beide Werthe von U sind auch durch $a=2$ theilbar, indem man hat $u=\frac{U}{2}=\pm 4$. Hieraus ergeben sich die beiden Auflösungen

$$x=\pm 4-3w$$
$$y=\ \ 3\mp 16w+6w^2$$

Einige spezielle Werthe dieser beiden Reihen sind

	für	$w=-2$	-1	0	1	2
1ste Reihe	$x=$	10	7	4	1	-2
	$y=$	59	25	3	-7	-5
2te Reihe	$x=$	2	-1	-4	-7	-10
	$y=$	-5	-7	3	25	59

§. 131. *Auflösung des allgemeinen Falles mit der Determinante null.*

Die gegebene Gleichung sei in die Form

(1) $$ax^2-2bxy-cy^2+2dx+2ey=k$$

gebracht, worin die Koeffizienten der Glieder in xy, x, y paare Zahlen sind. Nach der Voraussetzung ist

(3) $$D=b^2+ac=0 \text{ also } -ac=b^2$$

Wir nehmen an, dass das in xy multiplizirte Glied wirklich existire, dass also nicht $b=0$, folglich auch weder $a=0$, noch $c=0$ sei. Wäre das Letztere der Fall; so würde man nach §. 132 zu verfahren haben.

Ferner nehmen wir an, dass nicht $ae+bd=0$, mithin auch nicht $be-cd=0$ sei. Wäre Dies der Fall; so würde man nach §. 133 zu verfahren haben.

Multiplizirt man die gegebene Gleichung mit a; so lässt sie sich in die Form

$$(ax - by)^2 + 2a(dx + ey) = ak$$

oder wenn man

(3) $$z = ax - by$$

setzt, in die Form

(4) $$z^2 + 2a(dx + ey) = ak$$

bringen. Eliminirt man aus den beiden Gleichungen (3) und (4) erst y und dann x; so ergibt sich, wenn man zur Abkürzung

(5) $$X = -bz + ae$$

(6) $$Y = z + d$$

setzt,

(7) $$x = \frac{a^2(e^2 - ck) - X^2}{2ab(ae + bd)}$$

(8) $$y = \frac{(d^2 + ak) - Y^2}{2(ae + bd)}$$

Jetzt hat man für X und Y solche Werthe, welche wegen (5) und (6) offenbar ganzzahlig sein müssen, zu ermitteln, wodurch x und y ganze Zahlen werden. Ausserdem müssen diese Werthe von X und Y von der Beschaffenheit sein, dass wenn man dieselben in die aus (5) und (6) sich ergebende Beziehung

(9) $$z = \frac{X - ae}{-b} = Y - d$$

substituirt, die beiden Ausdrücke $\frac{X - ae}{-b}$ und $Y - d$ Einunddieselbe ganze Zahl z darstellen.

Zu diesem Ende ermittelt man im Hinblick auf die Gl. (7) die Reihen der durch $2ab(ae + bd)$ theilbaren Zahlen J von der Form $a^2(e^2 - ck) - X^2$. Für irgend Eine dieser Reihen möge

(10) $$X = u \text{ und } x = \frac{a^2(e^2 - ck) - u^2}{2ab(ae + bd)} = v$$

sein: alsdann ist allgemein

(11) $$X = u + 2ab(ae + bd)w$$

(12) $$x = v - 2uw - 2ab(ae + bd)w^2$$

Ferner ermittelt man im Hinblick auf die Gl. (8) die Reihen der durch $2(ae + bd)$ theilbaren Zahlen J von der Form $(d^2 + ak) - Y^2$. Irgend Einer dieser Reihen möge der Werth

(13) $$Y = u' \text{ und } y = \frac{(d^2 + ak) - u'^2}{2(ae + bd)} = v'$$

entsprechen. Alsdann ist allgemein

(14) $$Y = u' + 2(ae + bd)w'$$

(15) $$y = v' - 2u'w' - 2(ae + bd)w'^2$$

In den vorstehenden Gleichungen bezeichnen w und w' beliebige ganze Zahlen.

Die Werthe von X und Y aus (11) und (14) müssen nun noch die Bedingung (9) erfüllen. Es sind also diejenigen dieser

Werthe zu bestimmen, für welche die beiden Ausdrücke $\frac{X-ae}{-b}$ und $Y-d$ einander gleich und ganze Zahlen werden. Es leuchtet ein, dass wenn sie gleich sind, sie auch nothwendig ganz sein werden, da $Y-d$ stets ganz ist. Demnach braucht bloss die Gleichheit $\frac{X-ae}{-b}=Y-d$ oder

$$X-ae=-bY+bd \text{ oder } X+bY=ae+bd$$

erfüllt zu sein. Substituirt man hierin die obigen allgemeinen Werthe für X und Y; so kommt nach gehöriger Reduktion

$$(16) \qquad aw+w'=\frac{ae+bd-(u+bu')}{2b(ae+bd)}=U$$

Hieraus folgt, dass nothwendig die rechte Seite dieser Gleichung, welche wir zur Abkürzung mit U bezeichnet haben, eine ganze Zahl sein muss, weil die linke Seite $aw+w'$ es ist. Demnach kombinirt man in dem Ausdrucke für U jeden zulässigen Werth von u mit jedem zulässigen Werthe von u' und ermittelt, welche Kombinationen U zu einer ganzen Zahl machen. Jeder so für U gefundene Werth ist brauchbar, und führt zu einer unendlichen Reihe von Auflösungen. Denn wenn U ganz ist; so wird die Gleichung $aw+w'=U$, worin w und w' zwei unbekannte, aber nothwendig ganze Zahlen sind, stets möglich sein. Man kann darin offenbar für w jede beliebige positive oder negative ganze Zahl setzen; w' ist alsdann

$$(17) \qquad w'=U-aw$$

Substituirt man diesen Werth für w' in den Ausdruck (15) für y und notirt der Vollständigkeit wegen nochmals die Gleichung (12) für x; so ergibt sich die Auflösung der Gl. (1) in der Form

$$(18) \qquad x=v-2uw-2ab(ae+bd)w^2$$

$$(19) \quad \begin{cases} y=v'-2u'U-2(ae+bd)U^2+2a[u'+2(ae+bd)U]w \\ \qquad -2a^2(ae+bd)w^2 \end{cases}$$

Beispiel 1: $3x^2-6xy+3y^2+10x-4y=11$

Hier ist $D=b^2+ac=3^2+3(-3)=0$, $ae+bd=3(-2)+3.5=9$, und die Gleichungen (7), (8) werden

$$x=\frac{333-X^2}{162}, \quad y=\frac{58-Y^2}{18}$$

Man findet 6 Reihen der durch 162 theilbaren Zahlen J von der Form $333-X^2$. Für dieselben ist

$$u= \qquad \pm 3 \quad \pm 51 \quad \pm 57$$

$$v=\frac{333-u^2}{162}= \qquad 2 \quad -14 \quad -18$$

Ferner findet man zwei Reihen der durch 18 theilbaren Zahlen J von der Form $58-Y^2$. Für dieselben ist

$$\begin{array}{rl} u' = & \pm 2 \\ v' = \dfrac{58 - u'^2}{18} = & 3 \end{array}$$

Damit nun nach Gl. (16) $U = \dfrac{9 - (u + 3u')}{54}$ eine ganze Zahl werde, sind von den vorstehenden Werthen von u und u' nur folgende zu gebrauchen, neben welchen wir sofort die entsprechenden Werthe von v, v', U notiren wollen.

$$\begin{array}{rrrr} u = & 3 & -51 & 57 \\ u' = & 2 & 2 & 2 \\ v = & 2 & -14 & -18 \\ v' = & 3 & 3 & 3 \\ U = & 0 & 1 & -1 \end{array}$$

Durch Substitution dieser Werthe in die Formeln (18), (19) ergeben sich folgende 3 Reihen von Auflösungen

$$\begin{array}{lrrrrr} w = \ldots & -2 & -1 & 0 & 1 & 2\ldots \\ \left\{\begin{array}{l} x = 2 - 6w - 162w^2 = \ldots \\ y = 3 + 12w - 162w^2 = \ldots \end{array}\right. & \begin{array}{r} -634 \\ -669 \end{array} & \begin{array}{r} -154 \\ -171 \end{array} & \begin{array}{r} 2 \\ 3 \end{array} & \begin{array}{r} -166 \\ -147 \end{array} & \begin{array}{r} -658\ldots \\ -621\ldots \end{array} \\ \left\{\begin{array}{l} x = -14 + 102w - 162w^2 = \ldots \\ y = -19 + 120w - 162w^2 = \ldots \end{array}\right. & \begin{array}{r} -866 \\ -897 \end{array} & \begin{array}{r} -278 \\ -301 \end{array} & \begin{array}{r} -14 \\ -19 \end{array} & \begin{array}{r} -74 \\ -61 \end{array} & \begin{array}{r} -458\ldots \\ -427\ldots \end{array} \\ \left\{\begin{array}{l} x = -18 - 114w - 162w^2 = \ldots \\ y = -11 - 96w - 162w^2 = \ldots \end{array}\right. & \begin{array}{r} -438 \\ -467 \end{array} & \begin{array}{r} -66 \\ -77 \end{array} & \begin{array}{r} -18 \\ -11 \end{array} & \begin{array}{r} -294 \\ -269 \end{array} & \begin{array}{r} -894\ldots \\ -851\ldots \end{array} \end{array}$$

Beispiel 2: $x^2 + 4xy + 4y^2 - 10x - 8y = 0$

Hier ist $D = b^2 + ac = 2^2 + 1(-4) = 0$, $ae + bd = 1.(-4) + (-2)(-5) = 6$; und die Gleichungen (7), (8) werden

$$x = \frac{16 - X^2}{-24}, \qquad y = \frac{25 - Y^2}{12}.$$

Es gibt 4 Reihen der durch 24 theilbaren Zahlen von der Form $16 - X^2$. Für dieselben ist

$$\begin{array}{rrr} u = & \pm 4 & \pm 8 \\ v = \dfrac{16 - u^2}{-24} = & 0 & 2 \end{array}$$

Ferner gibt es 4 Reihen der durch 12 theilbaren Zahlen von der Form $25 - Y^2$. Für dieselben ist

$$\begin{array}{rrr} u' = & \pm 1 & \pm 5 \\ v' = \dfrac{25 - u'^2}{12} = & 2 & 0 \end{array}$$

Die Grösse $U = \dfrac{6 - (u - 2u')}{-24}$ aus Gl. (16) wird aber nur eine ganze Zahl für folgende Werthe von u und u'.

$$\begin{array}{rrrrr} u = & 4 & -4 & 8 & -8 \\ u' = & -1 & -5 & 1 & 5 \\ v = & 0 & 0 & 2 & 2 \\ v' = & 2 & 0 & 2 & 0 \\ U = & 0 & 0 & 0 & -1 \end{array}$$

Dies liefert folgende 4 Reihen von Auflösungen

	$w = \ldots$	-2	-1	0	1	$2\ldots$
$\begin{cases} x = \\ y = \end{cases}$	$\begin{matrix} -8w+24w^2 = \ldots \\ 2-2w-12w^2 = \ldots \end{matrix}$	$\begin{matrix} 112 \\ 42 \end{matrix}$	$\begin{matrix} 32 \\ -8 \end{matrix}$	$\begin{matrix} 0 \\ 2 \end{matrix}$	$\begin{matrix} 16 \\ -12 \end{matrix}$	$\begin{matrix} 80\ldots \\ -50\ldots \end{matrix}$
$\begin{cases} x = \\ y = \end{cases}$	$\begin{matrix} 8w+24w^2 = \ldots \\ -10w-12w^2 = \ldots \end{matrix}$	$\begin{matrix} 80 \\ -28 \end{matrix}$	$\begin{matrix} 16 \\ -2 \end{matrix}$	$\begin{matrix} 0 \\ 0 \end{matrix}$	$\begin{matrix} 32 \\ -22 \end{matrix}$	$\begin{matrix} 112\ldots \\ -68\ldots \end{matrix}$
$\begin{cases} x = \\ y = \end{cases}$	$\begin{matrix} 2-16w+24w^2 = \ldots \\ 2+2w-12w^2 = \ldots \end{matrix}$	$\begin{matrix} 130 \\ -50 \end{matrix}$	$\begin{matrix} 42 \\ -12 \end{matrix}$	$\begin{matrix} 2 \\ 2 \end{matrix}$	$\begin{matrix} 10 \\ -8 \end{matrix}$	$\begin{matrix} 66\ldots \\ -42\ldots \end{matrix}$
$\begin{cases} x = \\ y = \end{cases}$	$\begin{matrix} 2+16w+24w^2 = \ldots \\ -2-14w-12w^2 = \ldots \end{matrix}$	$\begin{matrix} 66 \\ -22 \end{matrix}$	$\begin{matrix} 10 \\ 0 \end{matrix}$	$\begin{matrix} 2 \\ -2 \end{matrix}$	$\begin{matrix} 42 \\ -28 \end{matrix}$	$\begin{matrix} 130\ldots \\ -78\ldots \end{matrix}$

§. 132. *Fall, wo das Glied in xy fehlt.*

In diesem Falle, wo $b=0$, mithin wegen $b^2+ac=0$ auch noch entweder $a=0$ oder $c=0$ sein muss, sei $c=0$. Die gegebene Gleichung hat alsdann die Form

(1) $$ax^2+2dx+ey=k$$

worin nur der Koeffizient von x, nicht aber der von y eine paare Zahl zu sein braucht.

Multiplizirt man diese Gleichung mit a, und addirt auf beiden Seiten D^2; so nimmt sie, wenn man

(2) $$z=ax+d$$

setzt, die Form

(3) $$z^2+aey=d^2+ak$$

an. Aus diesen beiden Gleichungen folgt

(4) $$x=\frac{z-d}{a}$$

(5) $$y=\frac{(d^2+ak)-z^2}{ae}$$

Hierin sind für z solche ganze Werthe zu setzen, wodurch x und y ganze Zahlen werden. Zu diesem Ende ermittele man in bekannter Weise die Reihen der durch ae theilbaren Zahlen J von der Form $(d^2+ak)-z^2$. Findet man für irgend Eine Reihe dieser Art den Werth

(6) $$z=u \text{ und } y=\frac{(d^2+ak)-u^2}{ae}=v$$

so sind die allgemeinen Werthe von z und y

(7) $$z=u+aew$$

(8) $$y=v-2uw-aew^2$$

Damit nun auch nach Gl. (4) $x=\frac{z-d}{a}=\frac{u+aew-d}{a}$ $=\frac{u-d}{a}+ew$ eine ganze Zahl werde, sind nur diejenigen Werthe von u brauchbar, für welche

(9) $$U=\frac{u-d}{a}$$

eine ganze Zahl ist. Die Auflösung wird alsdann

(10) $$x = U + ew$$

(11) $$y = v - 2uw - aew^2$$

Beispiel: $3x^2 - 6x + 4y = 5$

Die Gl. (5) wird hier

$$y = \frac{24 - z^2}{12}$$

Es gibt 3 verschiedene Reihen der durch 12 theilbaren Zahlen J von der Form $24 - z^2$. Man hat für dieselben

$$u = \quad 0 \quad \pm 6$$
$$v = \frac{24 - u^2}{12} = 2 \quad -1$$

Nach Gl. (9) muss hier $U = \frac{u+3}{3}$ eine ganze Zahl sein. Dies ist für jeden Werth von u der Fall. Man hat also

$$u = 0 \quad 6 \quad -6$$
$$v = 2 \quad -1 \quad -1$$
$$U = 1 \quad 3 \quad -1$$

Hiernach erhält man folgende 3 Reihen von Auflösungen

		$w =$	... -2	-1	0	1	2 ...
$x =$	$1 + 4w$	$=$	... -7	-3	1	5	9 ...
$y =$	$2 - 12w^2$	$=$	... -46	-10	2	-10	-46 ...
$x =$	$3 + 4w$	$=$	... -5	-1	3	7	11 ...
$y =$	$-1 - 12w - 12w^2$	$=$	... -25	-1	-1	-25	-73 ...
$x =$	$-1 + 4w$	$=$	... -9	-5	-1	3	7 ...
$y =$	$-1 + 12w - 12w^2$	$=$	... -73	-25	-1	-1	-25 ...

§. 133. *Fall, wo $ae + bd = 0$ ist.*

Die gegebene Gleichung sei

(1) $$ax^2 - 2bxy - cy^2 + 2dx + 2ey = k$$

sodass also die Koeffizienten von xy, x, y paare Zahlen sind. Da hier $D = b^2 + ac = 0$ vorausgesetzt wird; so muss, wenn $ae + bd = 0$ ist, auch stets $be - cd = 0$ sein.

Multiplizirt man die vorstehende Gleichung mit a und addirt auf beiden Seiten d^2; so wird dieselbe

$$(ax - by + d)^2 = d^2 + ak$$

oder wenn man auf beiden Seiten die Quadratwurzel auszieht,

(2) $$ax - by + d = \pm\sqrt{d^2 + ak}$$

Hieraus folgt, dass wenn die gegebene Gleichung möglich sein soll, zuvörderst $d^2 + ak$ ein vollständiges Quadrat sein muss. Ist Dies der Fall; so zerfällt dieselbe in zwei unbestimmte Gleichungen vom ersten Grade, welche durch

(3) $$ax - by = -d \pm \sqrt{d^2 + ak}$$

dargestellt sind.

Beispiel: $9x^2 - 12xy + 4y^2 + 6x - 4y = 35$

Die Gl. (3) wird hier

$$9x-6y=-3\pm\sqrt{9.35+9}=-3\pm18$$

d. i., wenn man durch 3 dividirt,

$$3x-2y=5 \text{ oder } -7$$

Die erste und zweite dieser beiden Gleichungen vom ersten Grade hat resp. die Auflösungen

	$w=$	... -2	-1	0	1	2 ...
$\{x=$	$1+2w=$	... -3	-1	1	3	5 ...
$\{y=$	$-1+3w=$	... -7	-4	-1	2	5 ...
$\{x=$	$-1+2w=$	... -5	-3	-1	1	3 ...
$\{y=$	$2+3w=$	... -4	-1	2	5	8 ...

§. 134. ***Bemerkungen behuf thunlichster Vereinfachung der zur Auflösung einer quadratischen Gleichung mit zwei Unbekannten dienenden Rechnung.***

I. Es leuchtet ein, dass wegen der Mannichfaltigkeit der Operationen, welche behuf Auflösung der in diesem Abschnitte behandelten Gleichungen erforderlich sind, und wegen der Grösse der dabei leicht sich einstellenden Zahlen, ein möglichst übersichtlicher, handgerechter und einfacher Entwickelungsgang, welcher gleichwol das Problem in grösster Allgemeinheit erschöpft und die unendliche Menge spezieller Auflösungen systematisch nach der relativen Grösse, nach dem Zeichen und nach sonstigen wesentlichen Eigenschaften gruppirt, ein wesentliches Bedürfniss ist. Wir haben uns im Obigen bemühet, dieser Bedingung der praktischen Brauchbarkeit zu entsprechen, und zu dem Ende auch der Vereinfachung der Hülfsrechnungen in den früheren Abschnitten eine besondere Sorgfalt zugewandt.

Eine schon in §. 100 angemerkte, auch hier oftmals zur Abkürzung der Rechnung dienende Regel, besteht darin, dass man das Quadrat derjenigen Unbekannten, welches mit dem kleineren Koeffizienten behaftet ist, in das erste Glied ax^2 der Gleichung stelle.

Ausserdem aber müssen wir noch auf eine andere Vereinfachung in alle den Fällen der §§. 130 bis 133 aufmerksam machen, wo bei der Determinante $D=0$ eine Multiplikation der gegebenen Gleichung mit dem Koeffizienten a vorgeschrieben ist. Diese Multiplikation hat den Zweck, im ersten Gliede ein vollständiges Quadrat a^2x^2 herzustellen. Dies kann in den Fällen, wo der Koeffizient a einen quadratischen Faktor $\alpha^2>1$ enthält, wo also $a=\alpha^2 a'$ ist, mit kleineren Zahlen in der Weise geschehen, dass man die gegebene Gleichung mit dem nicht quadratischen Faktor von a, also mit a' multiplizirt. Es wird nicht schwer sein, für diese Voraussetzung die früher gefundenen Formeln zu korrigiren, besonders, wenn man be-

achtet, dass aus der Beziehung $D = b^2 + ac = b^2 + \alpha^2 a' c = 0$ die andere $\left(\frac{b}{\alpha}\right)^2 = -a'c$ folgt, wonach die Grösse b durch α theilbar sein muss, sodass man $b = \alpha b'$ oder $\frac{b}{\alpha} = b'$ setzen kann.

II. Unter diesen Umständen hat man für den allgemeinen Fall aus §. 131, nachdem mit α multiplizirt ist,

$$(\alpha a' x - b' y)^2 + 2a' (dx + ey) = a' k$$

und demnach statt der dortigen Gleichungen (5), (6), (7), (8)

$$X = -b' z + a' e \tag{5}$$

$$Y = \alpha z + d \tag{6}$$

$$x = \frac{a'^2 (e^2 - ck) - X^2}{2a' b' (\alpha a' e + b' d)} \tag{7}$$

$$y = \frac{(d^2 + ak) - Y^2}{2 (ae + bd)} \tag{8}$$

Aus den Gleichungen (5) und (6) folgt statt der Gl. (9)

$$z = \frac{X - a' e}{-b'} = \frac{Y - d}{\alpha} \tag{9}$$

Es ist also jetzt, wo weder $\frac{X - a' e}{-b'}$, noch $\frac{Y - d}{\alpha}$ unbedingt eine ganze Zahl ist, nicht hinreichend, dass zwischen diesen beiden Grössen Gleichheit gestiftet werde; es ist vielmehr besonders nothwendig, dafür zu sorgen, dass dieselben ganze Zahlen werden. Der allgemeine Ausdruck von Y ist der aus §. 131, Gl. (14). Soll also $\frac{Y - d}{\alpha}$ eine ganze Zahl sein; so muss

$$\frac{u' + 2 (ae + bd) w' - d}{\alpha} = \frac{u' - d}{\alpha} + 2 (\alpha a' e + b' d) w'$$

also $\frac{u' - d}{\alpha}$ eine solche sein. Demnach sind zuvörderst aus den Grössen u' diejenigen auszuheben, für welche $\frac{u' - d}{\alpha}$ eine ganze Zahl wird. Jetzt hat man, damit auch $\frac{X - a' e}{-b'}$ eine ganze Zahl werde, diejenigen Werthe von u auszulesen, für welche

$$\frac{u + 2a' b' (\alpha a' e + b' d) w - a' e}{-b'} = \frac{u - a' e}{-b'} + 2a' (\alpha a' e + b' d) w$$

also für welche $\frac{u - a' e}{-b'}$ eine ganze Zahl wird.

Aus diesen Werthen von u' und u sind diejenigen zu ermitteln, welche die beiden Ausdrücke in Gl. (9) einander gleich machen. Dies liefert, ähnlich wie in §. 131, die Bedingung

(16) $$a'w + w' = \frac{aa'e + b'd - (au + b'u')}{2b'(ae + bd)} = U$$

Es sind also nur diejenigen Werthe von u und u' brauchbar, für welche U eine ganze Zahl wird. Für dieselben hat man

(17) $$w' = U - a'w$$

und als Auflösung der gegebenen Gleichung

(18) $$x = v - 2uw - 2a'b'(ae + bd)w^2$$

(19) $$\begin{cases} y = v' - 2u'U - 2(ae + bd)U^2 + 2a'[u' + 2(ae + bd)U]w \\ \qquad - 2a'^2(ae + bd)w^2 \end{cases}$$

III. Zur Erläuterung des Vorstehenden wollen wir nochmals das Beispiel 2 aus §. 131 berechnen, indem wir darin die beiden Unbekannten x, y miteinander vertauschen. Dies gibt

$$4x^2 + 4xy + y^2 - 8x - 10y = 0$$

Rechnen wir jetzt nach der Vorschrift des §. 131; so werden die dortigen Gleichungen (7) und (8)

$$x = \frac{400 - X^2}{192} \qquad y = \frac{16 - Y^2}{-24}$$

Es gibt 16 Reihen der durch 192 theilbaren Zahlen von der Form $400 - X^2$. Für dieselben ist

$$u = \pm 4, \pm 20, \pm 28, \pm 44, \pm 52, \pm 68, \pm 76, \pm 92.$$

Ferner gibt es 4 Reihen der durch 24 theilbaren Zahlen von der Form $16 - Y^2$. Für dieselben ist $u' = \pm 4, \pm 8$

Damit nun $U = \dfrac{12 - (u - 2u')}{48}$ eine ganze Zahl werde, können folgende 16 Kombinationen gemacht werden

$u =$	20	−28	68	−76	4	−44	52	−92
$u' =$	4	4	4	4	−4	−4	−4	−4
$u =$	−20	28	−68	76	−4	44	−52	92
$u' =$	8	8	8	8	−8	−8	−8	−8

Dies führt zu sechszehn Reihen von Auflösungen, von denen wir hier nur die ersten vier notiren wollen.

$x =$	$-40w - 192w^2$	$-2 + 56w - 192w^2$	$-22 - 136w - 192w^2$	$-28 + 152w - 192w^2$
$y =$	$10 + 128w + 384w^2$	$3 - 64w - 384w^2$	$66 + 320w - 384w^2$	$42 - 256w - 384w^2$

Statt solcher sechszehn Auflösungen haben wir in §. 131 nur deren vier gefunden. In der That sind die eben entwickelten ersten vier Auflösungen sämmtlich in der einzigen

$$x = -2 - 14w - 12w^2$$
$$y = 2 + 16w + 24w^2$$

des §. 131 enthalten. Die Vielheit der gegenwärtigen Ausdrücke für die Auflösung Ein oder derselben Gleichung ist hier die Folge von der Voranstellung des mit dem grösseren Koeffizienten behafteten Quadrates.

Beachtet man, dass in der vorstehenden Gleichung $a = 4 = 2^2 . 1 = \alpha^2 a'$ ist, also einen quadratischen Faktor $\alpha = 2$ besitzt; so kann man darauf die im gegenwärtigen Paragraphen angedeutete Regel in Anwendung bringen. Hiernach hat man, indem $b = -2 = 2(-1) = \alpha b'$ ist, statt Gl. (7) und (8)

$$x = \frac{25 - X^2}{12}, \qquad y = \frac{16 - Y^2}{-24}$$

Es gibt 4 Reihen der durch 12 theilbaren Zahlen von der Form $25 - X^2$. Man hat für dieselben $u = \pm 1, \pm 5$,

Ferner gibt es 4 Reihen der durch 24 theilbaren Zahlen von der Form $16 - Y^2$. Für dieselben ist $u' = \pm 4, \pm 8$

Da $b' = -1$ und $\alpha = 1$ ist; so erkennt man, dass für jeden dieser Werthe sowol $\frac{u - a'e}{-b'}$, wie auch $\frac{u' - d}{\alpha}$ eine ganze Zahl ist. Es sind also aus der Gesammtheit der Werthe von u und u' diejenigen auszuwählen, für welche nach Gl. (16)

$$U = \frac{-6 - 2u + u'}{24}$$

eine ganze Zahl wird. Dies gibt folgende vier Kombinationen

$u =$	-1	-5	1	-5
$u' =$	4	-4	8	-8
$U =$	0	0	0	-1
$v = \frac{25 - u^2}{12} =$	2	0	2	0
$v' = \frac{16 - u'^2}{-24} =$	0	0	2	2

Hierdurch erhält man **vier** Auflösungen, welche genau dieselben Reihen wie die bereits in §. 131 gefundenen darstellen.

Die Berücksichtigung des quadratischen Faktors von a hat also im Resultate den Effekt der Voranstellung des grösseren Koeffizienten wieder ausgeglichen.

Die

unbestimmte Analytik.

Von

Dr. Hermann Scheffler.

Zweite Abtheilung.

Hannover.
Im Verlage der Helwing'schen Hofbuchhandlung.
1854.

Druck von Ph. C. Göhmann.

Sechster Abschnitt.

Die Kongruenz der Zahlen.

---

§. 135. *Grundbegriffe und Grundformeln der Kongruenz der Zahlen.*

I. Die von Gauss in dem berühmten Werke *Disquisitiones arithmeticae* zur Begründung der Kongruenz der Zahlen eingeführte Formel

(1) $$a \equiv b \bmod p$$

bedeutet, dass die Differenz $a - b$ der beiden ganzen Zahlen a, b durch die ganze Zahl p theilbar sei, oder dass sich die beiden Zahlen a und b nur durch irgend ein Vielfaches der Zahl p von einander unterscheiden.

Die beiden Zahlen a und b heissen kongruent nach dem Model p. b heisst der Rest von a, und auch a der Rest von b. Von zwei nicht kongruenten Zahlen heisst die Eine der Nichtrest der anderen. Die Formel (1) heisst eine Kongruenz, und es ist klar, dass dieselbe nur ein einfacherer Ausdruck für die Gleichung

(2) $$a - b = np \text{ oder } a = np + b$$

ist, worin n irgend eine ganze Zahl bedeutet.

So hat man z. B.

$17 \equiv 2 \bmod 5$, weil $17 = 3.5 + 2$ ist
$17 \equiv 17 \bmod 5$, „ $17 = 0.5 + 17$ „
$17 \equiv 22 \bmod 5$, „ $17 = -1.5 + 22$ „
$17 \equiv -3 \bmod 5$, „ $17 = 4.5 - 3$ „
$-17 \equiv 3 \bmod 5$, „ $-17 = -4.5 + 3$ „
$-17 \equiv -7 \bmod 5$, „ $-17 = -2.5 - 7$ „
$17 \equiv 2 \bmod -5$, „ $17 = -3(-5) + 2$ „
$17 \equiv 0 \bmod 17$, „ $17 = 1.17 + 0$ „

Einer jeden Zahl a entsprechen für denselben Model p unendlich viel verschiedene kongruente Zahlen oder Reste b, welche

sowol positiv, wie negativ sein können. In zusammenhängender Reihe geschrieben, bilden je zwei benachbarte Reste die Differenz p. Unter allen diesen Resten ist zunächst der kleinste positive und der kleinste negative Rest von Wichtigkeit. Beide sind die einzigen, welche absolut genommen kleiner als der absolute Werth des Models p sind; sie bilden die Differenz p miteinander, insofern sie nicht beide $= 0$ sind.

Wenn diese beiden Reste, ohne Rücksicht auf das Zeichen, nicht beide $= \frac{p}{2}$ sind; so ist der Eine $< \frac{p}{2}$ und der andere $> \frac{p}{2}$.

Der absolut kleinere dieser beiden Reste, ohne Rücksicht auf das Zeichen, hat ebenfalls eine besondere Wichtigkeit, und heisst der absolut oder numerisch kleinste Rest.

Es wird in jedem speziellen Falle leicht sein, den Einen oder anderen der zuletzt genannten Reste zu bestimmen, wenn man beachtet, dass wegen $\frac{a}{p} = n + \frac{b}{p}$ für den Einen Rest die Grösse n der grösste Subquotient und für den anderen Rest die Grösse n der kleinste Superquotient des Bruches $\frac{a}{p}$ ist.

Bei den folgenden einfachen Sätzen, welche sich mit Hülfe der Gleichungen (2) leicht erweisen lassen, sollen sich die vorkommenden Kongruenzen, wenn das Gegentheil nicht ausdrücklich bemerkt ist, auf Ein und denselben Model p beziehen, weshalb wir der Einfachheit wegen den Zusatz *mod p* unterdrücken werden.

II. Jedes gemeinschaftliche Maass, welches in der Kongruenz (1) die beiden Grössen a und p besitzen, haben auch die beiden Grössen b und p miteinander gemein. Wenn a und p relativ prim sind, sind es auch b und p.

III. Die beiden Seiten einer Kongruenz können mit einander vertauscht werden. Wenn also $a \equiv b$; so ist auch $b \equiv a$ (natürlich für denselben Model).

IV. Es kann auf jeder Seite einer Kongruenz dieselbe Zahl c addirt oder subtrahirt werden. Wenn also $a \equiv b$; so ist auch $a \pm c \equiv b \pm c$. Hieraus folgt, dass die Glieder einer Kongruenz wie bei Gleichungen transponirt werden können. Ist also $a + c \equiv b$; so ist auch $a \equiv b - c$. Hiernach kann man jede Kongruenz $a \equiv b$ in der Form $a - b \equiv 0$ nach der Art der Gleichungen auf null reduciren. Auch folgt aus diesem Satze in Verbindung mit dem vorhergehenden, dass die Zeichen aller Glieder auf beiden Seiten einer Kongruenz umgekehrt werden können. Wenn also $a \equiv b$; so ist auch $-a \equiv -b$.

V. Beide Seiten einer Kongruenz können mit derselben Zahl multiplizirt werden. Wenn also $a \equiv b$; so ist auch $ac \equiv bc$.

VI. Dividirt können beide Seiten einer Kongruenz durch einen ihnen gemeinschaftlichen Faktor c stets dann werden, wenn c relativ prim zum Model ist. Denn wenn $ac \equiv bc$ oder $ac = np + bc$ ist; so ist offenbar das Glied np durch c theilbar. Ist nun c prim zu p; so muss n für sich durch c theilbar, also $\frac{n}{c}$ eine ganze Zahl sein. Es ist also wegen $a = \frac{n}{c} . p + b$ auch $a \equiv b$; folglich kann $ac \equiv bc$ durch c dividirt werden. Dies ist jedoch im Allgemeinen unstatthaft, wenn c und p ein gemeinschaftliches Maass besitzen.

VII. Zwei auf denselben Model sich beziehende Kongruenzen können wie zwei Gleichungen zu einander addirt oder von einander subtrahirt werden. Wenn also $a \equiv b$ und $c \equiv d$; so ist auch $a \pm c \equiv b \pm d$. Demnach können auch mehrere Kongruenzen addirt werden.

VIII. Zwei auf denselben Model sich beziehende Kongruenzen können miteinander multiplizirt werden. Wenn also $a \equiv b$ und $c \equiv d$; so ist auch $ac \equiv bd$. Durch Multiplikation mit $c = -1$ folgt hieraus nochmals der schon sub IV. angeführte Satz, dass die Zeichen aller Glieder auf beiden Seiten einer Kongruenz umgekehrt werden können. Es ist klar, dass auch mehrere derartige Kongruenzen mit einander multiplizirt werden können.

IX. Eine Kongruenz kann auf jede Potenz mit positivem ganzen Exponenten erhoben werden. Wenn also $a \equiv b$ und m eine positive ganze Zahl ist; so hat man auch $a^m \equiv b^m$. Dieser Satz ist eine unmittelbare Folge aus dem vorhergehenden.

X. Dividirt kann eine Kongruenz $ac \equiv bd$ durch eine andere $c \equiv d$, deren Seiten Faktoren der Seiten der ersteren sind, stets dann werden, wenn c und p, also auch d und p relativ prim sind. Denn aus $c \equiv d$ folgt durch Multiplikation mit a die Kongruenz $ac \equiv ad$, also wegen der anderen gegebenen Kongruenz $ac \equiv bd$ die fernere Kongruenz $ad \equiv bd$. Diese kann, wenn d und p relativ prim sind, nach VI durch d dividirt werden, und Dies gibt $a \equiv b$. Es kann also in diesem Falle $ac \equiv bd$ durch $c \equiv d$ dividirt werden. Besässe aber c und p, also auch d und p ein gemeinschaftliches Maass; so würde diese Division im Allgemeinen nicht zulässig sein.

XI. Für jeden Faktor irgend eines vollen Gliedes auf irgend einer Seite einer Kongruenz kann man, wenn der zweite Faktor, welcher mit jenem ersteren das fragliche Glied bildet, eine ganze Zahl ist, eine ihm nach demselben Model kongruente

Zahl substituiren. Wenn z. B. $A + aB \equiv C$ und für denselben Model $a \equiv b$; so ist, insofern B eine ganze Zahl darstellt, auch $A + bB \equiv C$. Denn aus $a \equiv b$ folgt $aB \equiv bB$. Subtrahirt man diese Kongruenz von der zuerst gegebenen; so kommt $A \equiv C - bB$ oder $A + bB \equiv C$.

Demnach kann man auch für jede positive ganze Potenz einer Grösse, welche den Faktor eines vollen Gliedes ausmacht, insofern der zweite Faktor eine ganze Zahl ist, dieselbe Potenz einer anderen Grösse substituiren, welche der ersteren nach demselben Model kongruent ist. Wäre also $a + bx^m \equiv C$ und $x \equiv y$, auch b eine ganze und m eine positive ganze Zahl; so hätte man ebenfalls $a + by^m \equiv C$.

Hieraus folgt, dass man in jeder Kongruenz, deren Seiten ganze rationale Funktionen von lauter ganzen Zahlen darstellen, welche also die allgemeine Form

$$a^\alpha b^\beta c^\gamma \ldots + d^\delta e^\varepsilon f^\varphi \ldots + \text{etc.}$$

besitzen, für jede Grösse, wie $a, b, \ldots$ oder auch für jede Grösse wie a^α, b^β oder wie $a^\alpha b^\beta$ u. s. w., welche den Faktor eines vollen Gliedes oder ein solches Glied selbst ausmacht, eine ihr nach demselben Model kongruente Zahl, oder überhaupt einen ihr kongruenten ähnlich gebildeten Ausdruck substituiren könne.

Wäre also eine solche Kongruenz in der Form

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0$$

gegeben; so könnte man stets zur Erzielung möglichst *kleiner* Zahlen für die Koeffizienten $a_0, a_1 \ldots a_n$ ihre kleinsten Reste in Beziehung zu demselben Model setzen. So hätte man z. B. statt

$$15x^4 + 7x^3 - 23x^2 + 17x - 8 \equiv 0 \ mod\ 7$$

auch die folgende Kongruenz mit absolut kleinsten Koeffizienten

$$x^4 - 2x^2 + 3x - 1 \equiv 0 \ mod\ 7$$

oder wenn man nur positive Koeffizienten haben wollte, folgende Kongruenz mit kleinsten positiven Koeffizienten

$$x^4 + 5x^2 + 3x + 6 \equiv 0 \ mod\ 7.$$

XII. Unter p unmittelbar aufeinander folgenden ganzen Zahlen $b, b+1, b+2 \ldots b+p-1$ kommt immer Eine, aber auch nur Eine Zahl vor, welche einer gegebenen Zahl a nach dem Model p kongruent ist. Demnach gibt es sowol unter den p Zahlen $0, 1, 2 \ldots p-1$, wie auch unter den p Zahlen $0, -1, -2 \ldots -(p-1)$ stets eine zu a nach dem Model p kongruente Zahl. Dies ist resp. der kleinste positive und negative Rest von a.

Von solchen p aufeinander folgenden Zahlen sind also keine zwei nach dem Model p einander kongruent.

Fern folgt hieraus, dass sowol die kleinsten positiven, wie

auch die kleinsten negativen Reste von zwei kongruenten Zahlen einander gleich sind. So ist z. B. für den Model 7 der kleinste positive Rest der Zahlen 9, 16 und -12, welche nach jenem Model einander kongruent sind, $=2$, und der kleinste negative Rest $=-5$.

XIII. Wenn der Model p den Werth 0 haben sollte; so bemerkt man leicht, dass dann jede Zahl a nur sich selbst kongruent sein kann, wodurch der Satz XII und der über die kleinsten Reste eine Änderung erleidet.

Wäre der Model $p=+1$; so würden alle obigen Sätze Gültigkeit behalten. Man erkennt aber, dass alsdann eine Zahl a jeder andern b kongruent ist.

XIV. Zwei Zahlen, welche nach einem gewissen Model kongruent sind, sind es auch nach jedem Faktor dieses Models. Man kann also in jeder Kongruenz für den Model Einen seiner Faktoren setzen. Wenn mithin $a \equiv b \bmod pq$; so ist auch $a \equiv b \bmod p$ und auch $a \equiv b \bmod q$.

XV. Wenn a zu b sowol nach dem Model p, als auch nach dem Model q kongruent ist, und p und q relativ prim sind; so ist auch a zu b nach dem Produkte pq kongruent. Wenn also unter dieser Voraussetzung $a \equiv b \bmod p$ und $a \equiv b \bmod q$; so ist auch $a \equiv b \bmod pq$.

Denn vermöge der gegebenen Kongruenzen ist $a-b$ sowol durch p, als auch durch q theilbar. Hieraus, und da p und q relativ prim sein sollen, folgt, dass $a-b$ durch pq theilbar, dass also $a \equiv b \bmod pq$ sei.

Zusatz. Wären a und b nach beliebig vielen Modeln $p, q, r \ldots$, von denen je zwei relativ prim sind, kongruent; so folgt aus vorstehendem Satze, dass auch $a \equiv b \bmod (pqr\ldots)$ sei.

XVI. Wenn a zu b nach dem Model p^n kongruent ist; so ist a^p zu b^p nach dem Model p^{n+1} kongruent. Wenn man also $a \equiv b \bmod p^n$ hat; so ist auch $a^p \equiv b^p \bmod p^{n+1}$.

Denn nach der gegebenen Kongruenz ist

$$a = b + vp^n$$

Erhebt man diese Gleichung auf die Potenz vom Grade p; so kommt, wenn $\overset{p}{B}_r$ den $r$ten Binomialkoeffizienten der $p$ten Potenz bezeichnet,

$$a^p = b^p + pb^{p-1}vp^n + \overset{p}{B}_2 b^{p-2}v^2p^{2n} + \ldots + v^p p^{pn} = b^p + wp^{n+1}$$

folglich $a^p \equiv b^p \bmod p^{n+1}$.

Zusatz 1. Aus vorstehendem Satze ergibt sich durch mehrmalige Anwendung des in ihm liegenden Gesetzes der folgende. Wenn $a \equiv b \bmod p^n$; so ist auch $a^{p^\alpha} \equiv b^{p^\alpha} \bmod p^{\alpha+n}$.

Zusatz 2. Von diesem Satze ist der nachstehende eine Spezialität, welche sich herausstellt, wenn man $n = 1$ annimmt.

Wenn $a \equiv b \mod p$; so ist auch $a^{p^\alpha} \equiv b^{p^\alpha} \mod p^{\alpha+1}$.

XVII. Wenn A zu B sowol nach dem Model P, als auch nach dem Model Q kongruent ist, und m das grösste gemeinschaftliche Maass von P und Q darstellt; so ist auch die $m$te Potenz von A der $m$ten Potenz von B nach dem Producte PQ jener beiden Model kongruent. Wenn also

$$A \equiv B \mod P \text{ und } A \equiv B \mod Q$$

so ist auch

$$A^m \equiv B^m \mod PQ.$$

Denn wenn $p, q, r \ldots$ lauter verschiedene Primzahlen sind; so können jede zwei beliebige Zahlen P und Q in der Form

$$P = p^a q^b r^c \ldots, \qquad Q = p^\alpha q^\beta r^\gamma \ldots$$

dargestellt werden, worin die Exponenten $a, b, c \ldots, \alpha, \beta, \gamma \ldots$ positive ganze Zahlen sind, unter welchen auch der Werth null vorkommen kann. Es wird nun der Exponent irgend eines Grundfaktors in der Zahl P entweder grösser oder kleiner oder gleich dem Exponenten desselben Grundfaktors der Zahl Q sein.

Wäre z. B. für den Grundfaktor p der Exponent $a > \alpha$; so schliesst man, dass weil p^a ein Faktor von P ist, wegen der ersten der beiden gegebenen Kongruenzen, nach dem Satze XIV, $A \equiv B \mod p^a$ sein wird. Hieraus und aus XVI, Zusatz 1, folgt

$$A^{p^\alpha} \equiv B^{p^\alpha} \mod p^{a+\alpha}$$

Wäre für den Grundfaktor q der Exponent $b < \beta$; so folgt aus der zweiten der beiden gegebenen Kongruenzen $A \equiv B \mod q^\beta$ und alsdann aus XVI, Zusatz 1

$$A^{q^b} \equiv B^{q^b} \mod q^{b+\beta}$$

Wäre für den Grundfaktor r der Exponent $c = \gamma$; so ist es gleichgültig, ob man aus der ersten der beiden gegebenen Kongruenzen den Schluss $A \equiv B \mod r^c$ oder aus der zweiten den Schluss $A \equiv B \mod r^\gamma$ ableitet, beide führen zu der Beziehung

$$A^{r^\gamma} \equiv B^{r^\gamma} \mod p^{c+\gamma}$$

Potenzirt man jede der so gewonnenen Kongruenzen nach IX dergestalt, dass der Exponent von A und B immer den Werth $p^\alpha q^b c^\gamma \ldots$, welcher offenbar gleich dem grössten gemeinschaftlichen Maasse m von P und Q ist, annimmt, indem man die zuerst gefundene Kongruenz auf den Grad $q^b r^\gamma \ldots$, die zweite auf den Grad $p^\alpha r^\gamma \ldots$, die dritte auf den Grad $p^\alpha q^b \ldots$ u. s. w. erhebt; so kommt

$$A^m \equiv B^m \mod p^{a+\alpha}, \quad A^m \equiv B^m \mod q^{b+\beta}, \quad A^m \equiv B^m \mod r^{c+\gamma}$$

u. s. w. Da nun $p, q, r \ldots$ lauter verschiedene Primzahlen, also von den Modeln $p^{a+\alpha}$, $q^{b+\beta}$, $r^{c+\gamma}$ etc. je zwei relativ prim sind; so folgt aus XV

$$A^n \equiv B^m \ mod(p^{a+\alpha} q^{b+\beta} r^{c+\gamma} \ldots) \quad \text{d. i.} \quad A^n \equiv B^m \ mod \ PQ$$

was zu beweisen war.

Zusatz. Wenn Q in P enthalten ist; so stellt Q selbst das grösste gemeinschaftliche Maass von P und Q dar und man hat $A^Q \equiv B^Q \ mod \ PQ$.

XVIII. Wenn der Model p eine Primzahl ist; so hat man stets

$$(a+b+c+\ldots)^p \equiv a^p + b^p + c^p + \ldots \ mod \ p$$

Denn nach dem binomischen Lehrsatze ist zunächst

$$(a+b)^p = a^p + B_1 a^{p-1} b + B_2 a^{p-2} b^2 + \ldots + B_{p-1} a b^{p-1} + b^p$$

Jeder Binomialkoeffizient, mit Ausnahme des vom Zeiger 0 und des vom Zeiger p, welche beide $= 1$ sind, ist durch p theilbar. Denn jeder dieser Koeffizienten, wie

$$B_n = \frac{p(p-1)(p-2)\ldots(p-n+1)}{1 \cdot 2 \cdot 3 \ldots n}$$

enthält im Zähler den Faktor p. Da nun p eine Primzahl und immer $> n$ ist; so kann keiner der im Nenner vorkommenden Faktoren 1, 2, 3 ... n darin aufgehen; es muss vielmehr der Nenner in dem Faktor $(p-1)(p-2)\ldots(p-n+1)$ des Zählers aufgehen, also B_n durch p theilbar sein.

Wenn hiernach $B_1 \equiv B_2 \equiv B_3 \equiv \ldots \equiv B_{p-1} \equiv 0 \ mod \ p$ ist; so folgt

$$(a+b)^p \equiv a^p + b^p$$

Hieraus ergibt sich

$$(a+b+c)^p \equiv (a+b)^p + c^p \equiv a^p + b^p + c^p \ mod \ p$$

u. s. w. für beliebig viele Glieder des Polynoms $a+b+c+\ldots$

§. 136. *Die Reste der sukzessiven Vielfachen einer gegebenen Zahl.*

I. Bestimmen wir die kleinsten positiven Reste der Zahlen $0.a$, $1a$, $2a$, $3a$, $4a \ldots$ nach dem Model p. Dieselben werden sämmtlich numerisch $< p$ sein, und wenn man sie mit r_0, r_1, r_2, r_3, $r_4 \ldots$ bezeichnet; so hat man

$$\begin{aligned} 0.a &= v_0 p + r_0 \quad \text{oder} \quad & 0.a &\equiv r_0 \equiv 0 \\ 1a &= v_1 p + r_1 & 1a &\equiv r_1 \\ 2a &= v_2 p + r_2 & 2a &\equiv r_2 \\ &\vdots & &\vdots \end{aligned}$$

Die Reste r_0, r_1, $r_2 \ldots$, wovon offenbar der erste $r_0 = 0$ ist, findet man entweder, indem man die Grössen $0.a$, $1a$, $2a \ldots$ berechnet und jede durch p dividirt, wobei man, jenachdem a und p positiv oder negativ sind, bald die grössten Subquotienten, bald die kleinsten Superquotienten zu nehmen hat, oder einfacher, indem man, nachdem r_1 gefunden ist, nach und nach

$r_1 + r_1$, darauf $r_2 + r_1$, darauf $r_3 + r_1$ u. s. w. bildet und durch p dividirt, um resp. r_2, r_3, r_4 u. s. w. herzustellen.

II. Aus dieser letzteren Beziehung erhellet, dass jeder vorhergehende Rest den unmittelbar nachfolgenden bedingt, dass also von einer Stelle n an, wo sich ein schon bei dem früheren Zeiger m da gewesener Rest wiederholen sollte, auch alle späteren Reste in derselben Reihenfolge wiederholen müssen, sodass man resp. $r_m, r_{m+1}, r_{m+2} \ldots = r_n, r_{n+1}, r_{n+2} \ldots$ haben würde. In der That muss aber endlich einmal ein früherer Rest sich wiederholen, da sie alle $< p$ sind. Auch erkennt man, dass der erste Rest $r_0 = 0$ sich nothwendig bei dem Gliede

$$pa = ap + 0 \text{ oder } pa \equiv r_p = 0$$

aufs neue einstellen wird.

Demnach bilden die Reste $r_0, r_1, r_2 \ldots$ eine wiederkehrende Periode.

III. Was die Länge oder Gliederzahl dieser Periode betrifft; so kann sie, da $r_p = r_0 = 0$ das Anfangsglied irgend einer späteren Periode ist, nur $= p$ oder gleich einem Faktor von p sein.

Ist nun p eine Primzahl; so hat dieselbe keine Faktoren ausser 1 und p. Die Periode kann also dann entweder nur Ein Glied oder nur p Glieder besitzen. Man erkennt, dass eine eingliedrige Periode $r_0 = r_1 = r_2 \ldots = 0$ nur in dem Falle stattfindet, wo a ein Vielfaches von p ist.

Ist also p eine in a nicht aufgehende Primzahl; so besitzt die Periode der obigen Reste p Glieder. Da ein jeder Rest $< p$ ist, und in derselben Periode kein Rest zweimal vorkommen kann; so folgt, dass die Periode der fraglichen Reste alle Zahlen 0, 1, 2 ... $p-1$, wenn auch in einer anderen Reihenfolge, enthält.

Das letztere Gesetz findet auch dann noch statt, wenn p zwar zusammengesetzt, aber relativ prim zu a ist. Denn wäre alsdann die Gliederzahl der Periode $< p$; so müsste der Werth 0 unter den Resten $r_0, r_1, r_2 \ldots r_p$ ausser an beiden Enden r_0 und r_p noch irgend wo anders, etwa bei r_n vorkommen, sodass man also

$$na = v_n p + r_n = v_n p$$

hätte. Hiernach müsste na durch p theilbar sein; mithin, da a und p relativ prim sind, müsste n durch p theilbar sein. Das Letztere ist jedoch unmöglich, weil man $n < p$ hat. Demnach muss die Periode p Glieder umfassen.

IV. Wenn p mit a das grösste gemeinschaftliche Maass q besitzt, und man $a = a'q$, $p = p'q$ hat; so besitzt die

Periode der obigen Reste $\frac{p}{q} = p'$ Glieder. Der Rest null kehrt also dann zuerst bei dem Zeiger p' wieder. Denn untersucht man, welchen kleinsten Werth der Zeiger n in der Gleichung

$$na = v_n p \text{ d. i. hier } na'q = v_n p'q$$
$$\text{oder } na' = v_n p'$$

anzunehmen vermag; so leuchtet zuvörderst ein, dass weil a' und p' relativ prim sind, n durch p' theilbar sein muss. Der kleinste Werth von n, welcher > 0 ist, hat also den Betrag p'. Ausserdem leuchtet ein, dass jeder Rest r_n wegen der bestehenden Beziehung

$$na'q = v_n p'q + r_n$$

durch das grösste gemeinschaftliche Maass q von a und p theilbar ist, dass also alle Reste das gemeinschaftliche Maass q haben, und mithin kein Rest $= 1$ vorkommen kann.

Ferner folgt hieraus, dass weil es nur folgende p' Zahlen mit dem gemeinschaftlichen Maasse q gibt, welche $< p$ d. i. $< p'q$ sind:

$$0,\ q,\ 2q,\ 3q \ldots (p'-1)q$$

dass derjenige Rest, welcher zunächst > 0 ist, das grösste gemeinschaftliche Maass q der beiden Zahlen a und p darstellt. Dies gibt ein besonderes Mittel zur Bestimmung des grössten gemeinschaftlichen Maasses zweier Zahlen an die Hand.

Es leuchtet ein, dass der letztere Fall als der allgemeinere alle vorhergehenden mit einschliesst.

V. Als Beispiele zu den vorstehenden Gesetzen mögen folgende dienen

$a = 15$, $p = 11$	$a = 15$, $p = 8$	$a = 15$, $p = 20$	$a = 15$, $p = 6$
$0.15 \equiv 0$	$0.15 \equiv 0$	$0.15 \equiv 0$	$0.15 \equiv 0$
$1.15 \equiv 4$	$1.15 \equiv 7$	$1.15 \equiv 15$	$1.15 \equiv 3$
$2.15 \equiv 8$	$2.15 \equiv 6$	$2.15 \equiv 10$	also ist auch 3 das grösste gem. Maass von 15 u. 6
$3.15 \equiv 1$	$3.15 \equiv 5$	$3.15 \equiv 5$	
$4.15 \equiv 5$	$4.15 \equiv 4$	also ist auch 5 das grösste gem. Maass von 15 u. 20	
$5.15 \equiv 9$	$5.15 \equiv 3$		
$6.15 \equiv 2$	$6.15 \equiv 2$		
$7.15 \equiv 6$	$7.15 \equiv 1$		
$8.15 \equiv 10$			
$9.15 \equiv 3$			
$10.15 \equiv 7$			

VI. Wenn man in einer Periode, deren letzter Rest r_{n-1} sei, sodass man $r_n = 0$ und $na \equiv 0$ hat, die Reste vom Ende gegen den Anfang hin betrachtet; so findet man, indem p den positiven Werth des Models bezeichnet, die Beziehung

(1) $r_{n-1} = p - r_1, \quad r_{n-2} = p - r_2, \quad r_{n-3} = p - r_3$, etc.
oder auch

(2) $$r_1 + r_{n-1} = r_2 + r_{n-2} = r_3 + r_{n-3} = \ldots = p$$

wonach sich immer zwei Reste derselben Periode, welche gleich weit von den Gliedern mit den Zeigern 0 und n abstehen, zu dem Werthe von p ergänzen, und mithin die zweite Hälfte dieser Reste aus der ersten Hälfte leicht durch Subtraktion von p gebildet werden kann.

Die allgemeine Richtigkeit dieser Beziehung erhellet, wenn man erwägt, dass man wegen

$$na \equiv 0 \text{ und}$$
$$ma \equiv r_m \text{ die Beziehung}$$
$$(n-m)a \equiv -r_m \equiv p - r_m$$

hat, dass also die Grösse $p - r_m$, da sie positiv und $< p$ ist, den Rest r_{n-m} darstellt.

VII. Addirt man die $p-1$ Gleichungen

$$1a = v_1 p + r_1$$
$$2a = v_2 p + r_2$$
$$\vdots$$
$$(p-1)a = v_{p-1} p + r_{p-1}$$

und bezeichnet die Summe der Quotienten $v_1 + v_2 + \ldots + v_{p-1}$ mit S; so hat man, wenn a und p relativ prim sind, weil alsdann unter den Resten $r_1, r_2, \ldots r_{p-1}$ alle ganzen Zahlen $1, 2 \ldots p-1$ vorkommen, also

(3) $$r_1 + r_2 + \ldots + r_{p-1} = 1 + 2 + \ldots + (p-1) = \frac{p(p-1)}{2}$$

ist,

$$\frac{p(p-1)}{2} a = S.p + \frac{p(p-1)}{2}, \text{ folglich}$$

(4) $$S = \frac{(a-1)(p-1)}{2}$$

Besitzen jedoch a und p das grösste gemeinschaftliche Maass q, sodass man $a = a'q$, $p = p'q$ hat, was der allgemeinere Fall ist; so würden, wenn man zu den obigen Gleichungen noch die identische $0.a = v_0 p + r_0 = 0.p + 0$ fügte, die Reste $r_0, r_1 \ldots r_{p-1}$ in q Perioden zerfallen. Jede dieser Perioden enthält die Zahlen $0.q, 1.q, 2q \ldots (p'-1)q$, deren Summe $= \frac{p'(p'-1)}{2} q = \frac{p(p'-1)}{2}$ ist.

Demnach ergibt für diesen Fall die obige Addition

$$\frac{p(p-1)}{2} a = S.p + \frac{p(p'-1)}{2} q, \text{ folglich}$$

(5) $$S = \frac{(a-1)(p-1) + q - 1}{2}$$

§. 137. **Kongruenzen vom ersten Grade mit Einer Unbekannten.**

Wenn in den Gliedern einer Kongruenz eine unbekannte Grösse x (welche stets als ganze Zahl gedacht wird) auf erster Potenz verflochten ist; so lässt sich dieselbe stets auf die einfache Form

(1) $$ax \equiv c \bmod p$$

zurückführen. Eine solche Kongruenz vom ersten Grade hat offenbar denselben Sinn, wie die unbestimmte Gleichung mit zwei Unbekannten x, y von der Form

(2) $$ax = py + c \text{ oder } ax - py = c$$

Was die Auflösung der Kongruenz (1), also die Ermittelung der für die Grösse x zulässigen Werthe betrifft; so könnte man zu diesem Ende die unbestimmte Gleichung (2) in bekannter Weise auflösen. Will man jedoch mehr in dem eigenthümlichen Geiste der Kongruenzen verfahren und dadurch umgekehrt noch eine neue Methode zur Auflösung der unbestimmten Gleichung (2) erhalten; so kann Dies folgendermaassen geschehen.

Zunächst leuchtet ein, dass man auf der rechten Seite der gegebenen Kongruenz (1) statt c immer dessen kleinsten positiven Rest r substituiren kann, welcher immer $< p$ sein wird, und welcher sich durch Division mit p in c ergibt. Dies sei geschehen; man habe also

(3) $$ax \equiv r \bmod p$$

Was das Kriterium der Möglichkeit oder Unmöglichkeit der gegebenen Kongruenz anlangt; so weiss man aus §. 136, dass wenn a und p relativ prim sind, die kleinsten Reste der Vielfachen von a, also der Grössen ax, jeden Werth der Zahlen $0, 1, 2 \ldots p$ annehmen können. Welchen Werth also die Grösse c oder r alsdann auch haben möge; die Kongruenz wird stets lösbar sein.

Besitzen jedoch a und p das gemeinschaftliche Maass q, indem man $a = a'q$ und $p = p'q$ hat; so muss nach §. 136 nothwendig auch r und nach §. 135, II. auch c dieses gemeinschaftliche Maass haben; es muss also $c = c'q$ und $r = r'q$ sein. Wäre Dies nicht der Fall; so läge eine unmögliche Kongruenz vor. Ist aber $c = c'q$; so hat man statt (1) und (2)

$$a'qx \equiv c'q \bmod p'q \text{ oder } a'qx = p'qy + c'q$$

also wenn man die letztere Gleichung mit q dividirt,

$$a'x \equiv c' \bmod p' \text{ oder } a'x = p'y + c'$$

welche Formeln durch dieselben Werthe von x und y erfüllt werden, wie die gegebenen (1) und (2), also für dieselben gesetzt werden können. Da nun a' und p' relativ prim sind; so ist die Aufgabe möglich.

Man sieht, dass die vorstehenden Bedingungen der Lösbarkeit mit den im zweiten Abschnitte gefundenen übereinstimmen. Im Übrigen stellt sich eine etwaige Unmöglichkeit bei der Anwendung der nahestehenden Methode von selbst heraus, auch wenn man nicht die eben bezeichnete Untersuchung über das gemeinschaftliche Maass von a und p voranschickt.

Zur Auflösung der Kongruenz (1) bildet man die erste Periode der kleinsten positiven Reste der sukzessiven Vielfachen von a. Kommt hierunter der kleinste Rest r nicht vor; so ist die Aufgabe unmöglich. Kommt derselbe dagegen vor; so kann Dies nur Ein Mal geschehen. Entspräche Dies dem $x_1$fachen von a; so hat man den kleinstmöglichen positiven Werth $x = x_1$ gefunden.

Besitzt die Periode der Reste n Glieder; so weiss man aus §. 136, dass derselbe Rest r den

$$\left.\begin{matrix} x_1, \; x_1+n, \; x_1+2n, \; x_1+3n, \ldots \\ x_1-n, \; x \;-2n, \; x_1-3n, \ldots \end{matrix}\right\} \text{fachen}$$

von a entspricht. Man hat also allgemein

$$(4) \qquad x = x_1 + nw$$

worin w jede willkürliche ganze Zahl darstellt.

Wenn a und p relativ prim sind, was man stets leicht von vorn herein erreichen kann; so ist $n = p$, also

$$(5) \qquad x = x_1 + pw$$

Die letztere Gleichung kann man in Form einer Kongruenz, nämlich als

$$x \equiv x_1 \; mod \, p$$

schreiben. Hieraus erkennt man, dass wenn a und p relativ prim sind, alle Auflösungen der Kongruenz (1) einander und zwar der Grösse x_1 in Beziehung zu demselben Model p kongruent sind, dass also eine Kongruenz vom ersten Grade nur Eine positive Auflösung oder Wurzel hat, welche kleiner als der numerische Werth des Models p ist.

Wir bemerken noch, dass Gauss die Wurzel der Kongruenz (1), analog der der Gleichungen, durch den Ausdruck $\frac{c}{a} mod\, p$ andeutet, sodass man allgemein $x \equiv \frac{c}{a} mod\, p$ schreiben kann.

Wenn man die Werthe von x kennt, welche der Kongruenz (1) oder der Gl. (2) entsprechen; so ergeben sich für die Gl. (2) die Werthe von y unter Zugrundelegung der Beziehung (4) durch

$$y = \frac{ax-c}{p} = \frac{x_1 a - c}{p} + \frac{na}{p} w$$

oder wenn man den Quotienten $\frac{x_1 a - c}{p} = y_1$ setzt,

(6) $$y = y_1 + \frac{na}{p} . w$$

Insofern a und p relativ prim sind, also $n = p$ ist, hat man

(7) $$y = y_1 + aw$$

Es gereicht der Rechnung zur Erleichterung, wenn man stets dafür sorgt, dass der Model p positiv sei. Dies kann stets geschehen, indem es offenbar thunlich ist, in der Gl. (2) zugleich die Zeichen von p und y umzukehren. Hätte man also zu diesem Zwecke statt eines negativen Models p dessen positiven Werth $-p$ genommen; so müsste man die Werthe von y in Gl. (5) oder (6) ebenfalls mit entgegengesetzten Zeichen nehmen.

Beispiel 1. Im ersten Beispiele des §. 29 war gegeben: $25x + 13y = 37$ oder

$$25x = -13y + 37 = 13(-y) + 37$$

Dies entspricht der Kongruenz

$$25x \equiv 37 \; mod \; 13$$

oder da der kleinste positive Rest von 37 gleich 11 ist,

$$25x \equiv 11 \; mod \; 13$$

Da 25 und 13 relativ prim sind; so ist die Aufgabe möglich, und wenn wir die erste Periode der Reste der sukzessiven Vielfachen von 25 bilden; so wird dieselbe 13 Glieder enthalten müssen. Wir werden also die Restbildung sofort abbrechen, sobald der gesuchte Rest 11 erschienen ist. Man hat

$$0.25 \equiv 0$$
$$1.25 \equiv 12$$
$$2.25 \equiv 11$$

folglich $x_1 = 2$ und nach Gl. (4)

$$x = 2 + 13w$$

Ferner nach Gl. (7), da $y_1 = \frac{x_1 a - c}{p} = \frac{2.25 - 37}{13} = 1$ ist, und in Erwägung, dass wir oben das Zeichen von p umgekehrt haben, dass also auch das von y umzukehren ist,

$$y = -1 - 25w$$

Die Formeln stellen genau dieselbe Zahlenreihe dar, wie die in §. 29 gefundenen.

Beispiel 2. Im zweiten Beispiele des §. 29 hatte man

$$23x = 15y + 30$$

Dies gibt die Kongruenz

$$23x \equiv 30 \; mod \; 15 \equiv 0 \; mod \; 15$$

Da 23 und 15 relativ prim sind, hat die Periode der Reste der Vielfachen von 23 genau 15 Glieder. Der kleinste Rest von $c = 30$, welcher $= 0$ ist, kommt bekanntlich bei $x_1 = 0$ vor. Wir haben also weiter keine Ermittelung nöthig. Es ist nach Gl. (5)

$$x = 15w$$

und nach Gl. (7), da $y_1 = \frac{x_1 a - c}{p} = \frac{0.23 - 30}{15} = -2$ ist,

$$y = -2 + 23w$$

Beispiel 3. Im zweiten Beispiele des §. 33 war die Gleichung

$$4x = 5y - 2$$

zu lösen. Dies entspricht der Kongruenz

$$4x \equiv -2 \; mod \; 5 \equiv 3 \; mod \; 5$$

Da 4 und 5 relativ prim sind, wird die Periode der Reste der Vielfachen von 4 im Ganzen 5 Glieder haben. Die Ermittelung derselben kann abgebrochen werden, sobald sich der kleinste positive Rest von -2, welcher $= 3$ ist, eingestellt hat. Hiernach ergibt sich

$$0.4 \equiv 0$$
$$1.4 \equiv 4$$
$$2.4 \equiv 3.$$

also $x_1 = 2$ und nach Gl. (5)

$$x = 2 + 5w$$

Ferner ist $y_1 = \frac{x_1 a - c}{p} = \frac{2.4 - (-2)}{5} = 2$, also nach Gl. (7)

$$y = 2 + 4w$$

Wir haben im Vorstehenden einige schon früher behandelte unbestimmte Gleichungen aufgelös't, um Gelegenheit zu einer Vergleichung der nach den verschiedenen Methoden aufzuwendenden Rechenarbeit zu geben. Es lässt sich nicht verkennen, dass die Kongruenzen ein elegantes und einfaches Mittel zur Auflösung jener Gleichungen darbieten. Um die Anzahl der zu bildenden Reste auf ein Minimum zu reduziren, ist es im Allgemeinen rathsam, den kleineren Koeffizienten der beiden Unbekannten x, y zum Model zu nehmen.

§. 138. *Zahlen, welche in einer gegebenen enthalten sind — welche relativ prim zu ihr sind — und welche ein gemeinschaftliches Maass mit ihr besitzen.*

I. Wenn $p, q, r \ldots$ die verschiedenen Primfaktoren einer Zahl a sind; so habe man

(1) $$a = p^\alpha q^\beta r^\gamma \ldots$$

Zur Bestimmung der verschiedenen Faktoren von a, hat man zuvörderst die Werthe $1, p, p^2 \ldots p^\alpha$, deren Anzahl $\alpha + 1$ ist.

Jeder dieser Werthe kann mit jedem der Werthe $1, q, q^2 \ldots q^\beta$, deren Anzahl $\beta + 1$ ist, kombinirt werden. Dies gibt $(\alpha + 1)(\beta + 1)$ Faktoren.

Jeder der so erhaltenen Werthe kann mit jedem der Werthe $1, r, r^2 \ldots r^\gamma$, deren Anzahl $\gamma + 1$ ist, kombinirt werden, wodurch $(\alpha + 1)(\beta + 1)(\gamma + 1)$ Faktoren entstehen.

Hieraus erkennt man, dass die Anzahl aller **verschiedenen Faktoren** von a

$$=(\alpha+1)(\beta+1)(\gamma+1)\ldots$$

ist. Hierunter sind auch die beiden Werthe 1 und a als Faktoren von a mitgerechnet.

So hat z. B. die Zahl 360, welche $=2^3.3^2.5$ ist, $4.3.2=24$ Faktoren.

II. Um die Anzahl der Zahlen zu ermitteln, welche **kleiner als a und relativ prim zu a** sind, eine Anzahl, welche wir kurz mit $\varphi(a)$ bezeichnen wollen, wobei wir den Werth 1 mit unter die zu a primen Zahlen rechnen; so leuchtet zuvörderst ein, dass wenn a eine Primzahl p ist, jede der Zahlen 1, 2, 3...$(p-1)$ relativ prim zu a sein wird, dass man also

(2) $$\varphi(p)=p-1$$

hat.

Wenn a die Potenz einer Primzahl, also $=p^\alpha$ ist, so sind alle diejenigen der Zahlen $1, 2, 3\ldots p^\alpha$ relativ prim zu a, welche übrig bleiben, wenn man die Werthe $p, 2p, 3p\ldots(p^{\alpha-1}p)$ ausscheidet. Da die Anzahl der letzteren $=p^{\alpha-1}$ ist; so ist die der ersteren $=p^\alpha-p^{\alpha-1}=(p-1)p^{\alpha-1}$. Man hat also

(3) $$\varphi(p^\alpha)=(p-1)p^{\alpha-1} \text{ oder auch}$$
$$=p^\alpha.\frac{p-1}{p}=a.\frac{p-1}{p}$$

Wenn a das Produkt aus zwei Primzahlen, also $=pq$ ist; so hat man aus den Zahlen $1, 2, 3\ldots(pq)$ zuvörderst die q Werthe $p, 2p, 3p\ldots qp$ und alsdann die p Werthe $q, 2q, 3q\ldots pq$ auszuscheiden. In diesen beiden Reihen haben nur die letzten Zahlen qp und pq Ein und denselben Werth, nämlich den Werth a. Alle übrigen sind verschieden: denn wäre $mp=nq$; so müsste, da p und q Primzahlen sind; q in m und p in n aufgehen, also da mp und nq nicht grösser als $a=pq$ sein kann, $m=q$ und $n=p$, folglich $mp=nq=a$ das letzte Glied in jeder der fraglichen beiden Reihen sein. Demnach ist die Anzahl der auszuscheidenden Werthe $=p+q-1$ und die der übrig bleibenden $=pq-(p+q-1)=(p-1)(q-1)$, Hiernach hat man

(4) $$\varphi(pq)=(p-1)(q-1) \text{ oder auch}$$
$$=pq.\frac{p-1}{p}.\frac{q-1}{q}=a.\frac{p-1}{p}.\frac{q-1}{q}.$$

Nehmen wir jetzt an, P sei irgend eine prime oder zusammengesetzte Zahl, p jedoch eine Primzahl; man sei im Stande, die Anzahl $\varphi(P)$ der zu P relativ primen Zahlen zu bestimmen, und gehe darauf aus, die Anzahl $\varphi(Pp)$ der zu Pp relativ primen Zahlen zu ermitteln.

Man bezeichne die zu P relativ primen Zahlen mit $b, c, d \ldots$, und trenne alle ganzen Zahlen von 1 bis Pp nach ihrer natürlichen Reihenfolge in p Gruppen, von denen jede P Zahlen, und zwar die erste die Zahlen $1, 2 \ldots P$, die zweite die Zahlen $P+1, P+2 \ldots 2P$ und irgend eine spätere die Zahlen $nP+1, nP+2 \ldots (n+1)P$ enthält. Ist nun p in P enthalten; so ist offenbar jede zu P relativ prime Zahl auch zu Pp relativ prim. Ferner ist klar, dass alsdann jede der genannten Gruppen gleich viel solcher zu P oder Pp relativ primer Zahlen enthält, denn in irgend einer mit $nP+1$ anhebenden Gruppe sind augenscheinlich die Zahlen $nP+b, nP+c, nP+d \ldots$, sonst aber keine zu P prim. Da nun die Anzahl der in der ersten Gruppe vorkommenden Zahlen dieser Art $= \varphi(P)$ ist; so ist die Anzahl aller zu P und demnach auch zu Pp primen Zahlen, welche $< Pp$ sind, wenn p in P aufgeht,

$$(5) \qquad \varphi(Pp) = p\,\varphi(P)$$

Ist dagegen p nicht in P enthalten; so sind aus den eben genannten Zahlen, welche relativ prim zu P sind, alle diejenigen auszuscheiden, welche Vielfache von p bilden. Dieses können aber nur die Zahlen $ar, br, cr \ldots$ sein, deren Menge $= \varphi(P)$ ist. Demnach hat man, wenn p nicht in P aufgeht

$$(6) \qquad \varphi(Pp) = p\,\varphi(P) - \varphi(P) = (p-1)\,\varphi(P)$$

Aus diesen beiden Beziehungen (5), (6) und aus (2) folgt sofort, dass wenn a die allgemeine Zusammensetzung (1) hat, die Anzahl der zu a relativ primen Zahlen, welche kleiner als a sind, durch

$$(7) \qquad \varphi(a) = p^{\alpha-1}(p-1)\,q^{\beta-1}(q-1)\,r^{\gamma-1}(r-1)\ldots$$

ausgedrückt ist. Dieser Ausdruck lässt sich auch in die Form

$$(8) \qquad \varphi(a) = a \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r} \ldots$$

stellen.

Aus (7) erkennt man auch, dass wenn sich die Zahl a in die Faktoren $P, Q, R \ldots$ zerlegen lässt, von welchen je zwei relativ prim sind, man

$$\varphi(PQR \ldots) = \varphi(P) \cdot \varphi(Q) \cdot \varphi(R) \ldots$$

hat.

Für die Zahl $360 = 2^3 . 3^2 . 5$ hat man nach (8)

$$\varphi(360) = 360 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 96$$

Wir machen noch darauf aufmerksam, dass die Anzahl der zu a relativ primen Zahlen (wennicht $a=2$) stets paar ist, dass die Hälfte derselben $< \frac{a}{2}$ und die andere Hälfte $> \frac{a}{2}$ ist, auch dass eine Zahl der ersten Hälfte mit derjenigen Zahl der zweiten Hälfte, welche ebensoweit von a absteht, als die erstere

von 0, die Summe a ausmacht, indem, wenn b irgend eine zu a relativ prime Zahl darstellt, auch $a-b$ eine solche ist.

III. Nachdem man in den Stand gesetzt ist, die Anzahl der zu a relativ primen Zahlen, welche $<a$ sind, zu bestimmen, **kann man auch leicht die Anzahl derer angeben, welche mit a ein gemeinschaftliches Maass besitzen.** Indem hiervon die Zahl 1 ausgeschlossen (also als eine zu a prime Zahl betrachtet wird), hat man für die gesuchte Anzahl nach (8)

$$(10) \qquad a-\varphi(a)=a\left(1-\frac{p-1}{p}\cdot\frac{q-1}{q}\cdot\frac{r-1}{r}\cdots\right)$$

Von diesen Zahlen gehen nach I. deren $[(\alpha+1)(\beta+1)(\gamma-1)\ldots]-1$ in a auf; die übrigen aber, deren Anzahl

$$a\left(1-\frac{p-1}{p}\cdot\frac{q-1}{q}\cdot\frac{r-1}{r}\cdots\right)-\left[(\alpha+1)(\beta+1)(\gamma+1)\ldots\right]+1$$

$$=a+1-a\left[\frac{p-1}{p}\cdot\frac{q-1}{q}\cdot\frac{r-1}{r}\cdots\right]-\left[(\alpha+1)(\beta+1)(\gamma+1)\ldots\right]$$

ist, gehen in a nicht auf, besitzen aber mit a ein gemeinschaftliches Maass.

Für die Zahl 360, für welche nach II. $\varphi(360)=96$ ist, gibt es also $360-96=264$ Zahlen, welche ein gemeinschaftliches Maass mit 360 besitzen. Hiervon gehen nach I. deren 23 in 360 auf, die übrigen 241 aber nicht.

IV. Wenn $f, f', f''\ldots$ die verschiedenen Faktoren von a nach I. sind (unter denen sich also auch der Werth 1 befindet); so hat man die Beziehung

$$(11) \qquad \varphi(f)+\varphi(f')+\varphi(f'')+\ldots=a$$

wobei zu bemerken ist, dass für $f=1$, $\varphi(1)=1$ und nicht $=0$ gedacht ist, sodass man also allgemein unter $\varphi(f)$ die Menge der zu f primen Zahlen versteht, welche nicht grösser als f sind.

Denn wenn die zu f primen Zahlen, welche nicht grösser als f sind, mit $b, c, d\ldots$, ferner die zu f' primen Zahlen, welche nicht grösser als f' sind, mit $b', c', d'\ldots$ u. s. w. bezeichnet werden; so multiplizire man die ersten mit $\frac{a}{f}$, die zweiten mit $\frac{a}{f'}$ u. s. w., bilde also die Zahlen

$\frac{ab}{f}, \frac{ac}{f}, \frac{ad}{f}\ldots$ deren Anzahl $=\varphi(f)$ ist

$\frac{ab'}{f'}, \frac{ac'}{f'}, \frac{ad'}{f'}\ldots$ „ „ $=\varphi(f')$ „

etc. etc.

Dass keine dieser Zahlen, wie z. B. $\frac{ab}{f}$, $>a$ ist, leuchtet

ein, da b nicht grösser als f ist. Es sind aber auch keine zwei einander gleich. Denn zunächst erhellet für zwei Zahlen Ein und derselben Reihe wie $\frac{ab}{f}$ und $\frac{ac}{f}$ die Unmöglichkeit einer solchen Gleichheit auf den ersten Blick. Was aber zwei Zahlen aus verschiedenen Reihen wie $\frac{ab}{f}$ und $\frac{ab'}{f'}$ betrifft; so würde die Gleichheit dieser beiden Zahlen die Gleichheit $bf' = b'f$ erfordern. Nun sind aber die beiden Zahlen f und f', als zwei verschiedene Faktoren von a, ungleich; es müsste also nothwendig irgend Einer von beiden, z. B. f, mit dem Koeffizienten b des anderen ein gemeinschaftliches Maass besitzen, was der Voraussetzung widerspricht, da b und f stets relativ prim sein sollen.

Endlich findet man, dass keine Zahl, welche den Werth a nicht übersteigt, unter den in Rede stehenden fehlen kann. Denn irgend eine die a nicht übersteigende Zahl sei $= p$. Dieselbe besitze mit a das grösste gemeinschaftliche Maass m, man habe also $a = mf$, $p = mb$, worin nun f ein Faktor von a und b eine zu f prime Zahl ist. Hiernach ergibt der Prozess, nach welchem die oberste Reihe der vorhin genannten Produkte gebildet ist, sofort im ersten Gliede die Zahl $\frac{ab}{f} = mb = p$.

Hiernach umfassen die beschriebenen Produkte alle a Zahlen $1, 2, 3 \ldots a$, und daraus folgt unmittelbar die Formel (11).

§. 139. *Der Fermatsche Lehrsatz.*

I. Unter diesem Namen ist folgender zuerst von Fermat aufgestellte Satz bekannt: Wenn p irgend eine in der positiven oder negativen Zahl a nicht enthaltene Primzahl ist, welche unbeschadet der Allgemeinheit der späteren Untersuchungen stets positiv gedacht werden kann; so ist $a^{p-1} - 1$ durch p theilbar.

Man hat also die Gleichung

(1) $$a^{p-1} - 1 = vp \text{ oder } a^{p-1} = vp + 1$$

oder auch die gleichbedeutende Kongruenz

(2) $$a^{p-1} \equiv 1 \mod p$$

Um diesen Satz zu beweisen, multipliziren wir von den in §. 136 gebildeten Kongruenzen, unter Ausschluss der obersten $0 . a \equiv 0$, die nächstfolgenden $p-1$, also die Kongruenzen

$$1a \equiv r_1$$
$$2a \equiv r_2$$
$$2a \equiv r_3$$
$$\vdots$$
$$(p-1)\, a \equiv r_{p-1}$$

mit einander. Dies gibt, wenn man erwägt, dass unter den $p-1$ kleinsten positiven Resten $r_1, r_2 \ldots r_{p-1}$ alle $p-1$ Zahlen $1, 2 \ldots (p-1)$ vorkommen,

$$1 . 2 . 3 . 4 \ldots (p-1) a^{p-1} \equiv 1 . 2 . 3 . 4 \ldots (p-1)$$

Da nun der Model p eine Primzahl ist, also mit dem Produkte $1 . 2 . 3 . 4 \ldots (p-1)$, dessen Faktoren sämmtlich kleiner als p, mithin relativ prim zu p sind, kein gemeinschaftliches Maass hat; so kann man die vorstehende Kongruenz nach §. 135, X. durch den beiderseitigen Koeffizienten $1 . 2 . 3 \ldots (p-1)$ dividiren. Dies gibt sofort den zu erweisenden Satz $a^{p-1} \equiv 1$.

So besteht z. B. für $a = 10$, $p \equiv 7$ die Kongruenz $10^6 \equiv 1 \; mod \, 7$ oder es ist $10^6 - 1 = 999999$ durch 7 theilbar.

II. Der Fermatsche Lehrsatz kann auch auf folgenden Satz gebracht werden: Wenn p eine in a nicht aufgehende Primzahl ist; so hat man für p als Model,

wenn $a \equiv 1$ ist,

$$(3) \qquad 1 + a + a^2 + \ldots + a^{p-1} = vp \text{ oder } \equiv 0$$

wenn a nicht $\equiv 1$ ist,

$$(4) \qquad 1 + a + a^2 + \ldots + a^{p-2} = vp \text{ oder } \equiv 0$$

Denn nach dem Fermatschen Lehrsatze hat man

$$(5) \qquad a^{p-1} - 1 = (a-1)(1 + a + a^2 + \ldots + a^{p-2}) \equiv 0$$

Nun ist, da p eine Primzahl darstellt, $a - 1$ entweder ein Vielfaches von p oder relativ prim zu p. Im ersten Falle ist $a - 1 \equiv 0$ oder $a \equiv 1$, folglich $1 \equiv 1$, $a \equiv 1$, $a^2 \equiv 1$, $a^3 \equiv 1 \ldots a^{p-1} \equiv 1$, mithin, wenn man die letzteren p Kongruenzen addirt

$$1 + a + a^2 + \ldots + a^{p-1} \equiv p \equiv 0$$

Im zweiten Falle dagegen kann man die Kongruenz (5) durch $a - 1$ dividiren. Dies gibt

$$1 + a + a^2 + \ldots + a^{p-2} \equiv 0$$

III. Aus dem Fermatschen Lehrsatze ergibt sich ferner für alle Primzahlen $p > 2$, welche also sämmtlich unpaar sind, sodass dafür $p - 1$ eine paare Zahl ist, der gleichfalls beachtenswerthe Satz

$$(6) \qquad a^{\frac{p-1}{2}} \equiv \pm 1$$

Denn nach dem Fermatschen Satze (2) hat man $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0$. Da der Model p eine Primzahl ist; so kann die letztere Kongruenz offenbar entweder nur dann bestehen, wenn der Faktor $a^{\frac{p-1}{2}} - 1 \equiv 0$, also $a^{\frac{p-1}{2}} \equiv 1$, oder wenn der Faktor $a^{\frac{p-1}{2}} + 1 \equiv 0$, also $a^{\frac{p-1}{2}} \equiv -1$ ist. Demnach muss die Potenz $a^{\frac{p-1}{2}}$ entweder $\equiv 1$ oder $\equiv -1$ sein.

§. 140. ***Verallgemeinerung des Fermatschen Lehrsatzes für den Fall, dass der Model keine Primzahl ist.***

A und P seien zwei beliebige Zahlen, und es sei zu untersuchen, welche Potenz von A zu der Zahl 1 nach dem Model P kongruent sein werde.

Zunächst erhellet, dass wenn A und P ein gemeinschaftliches Maass m haben, wenn also $A = am$, $P = pm$ ist, keine Potenz von A jene Eigenschaft besitzen kann. Denn sollte $(am)^x \equiv 1 \, mod \, pm$ sein; so müsste $a^x m^x - 1$ durch pm, also auch durch m theilbar sein. Da nun $a^x m^x$ durch m theilbar ist; so müsste es auch 1 sein, was unmöglich ist.

Wir beschränken also die Untersuchung auf den Fall, wo A und P relativ prim sind. Enthält nun P die Primfaktoren $p, q, r \ldots$, wovon keiner in A aufgehen wird, und ist demnach

(1) $$P = p^\alpha q^\beta r^\gamma \ldots,$$

so besteht der erweiterte Fermatsche Lehrsatz darin, dass wenn

(2) $$\varphi = (p-1)p^{\alpha-1}(q-1)q^{\beta-1}(r-1)r^{\gamma-1}\ldots$$

gesetzt wird,

(3) $$A^\varphi \equiv 1 \, mod \, P$$

ist. Aus §. 138, II. erhellet, dass φ die Anzahl der zu P relativ primen Zahlen, welche $< P$ sind, bezeichnet.

Zum Beweise dieses Satzes beachte man, dass nach dem vorhergehenden Paragraphen $A^{p-1} \equiv 1 \, mod \, p$ ist. Erhebt man diese Kongruenz auf die Potenz vom Grade $p^{\alpha-1}$; so folgt aus §. 135, XVI. $A^{(p-1)p^{\alpha-1}} \equiv 1 \, mod \, p^\alpha$

Ebenso ergibt sich $A^{(q-1)q^{\beta-1}} \equiv 1 \, mod \, q^\beta$, $A^{(r-1)r^{\gamma-1}} \equiv 1 \, mod \, r^\gamma$ u. s. w.

Potenzirt man jede dieser Kongruenzen dergestalt, dass der Exponent von A immer den Werth φ annimmt; so ergibt sich $A^\varphi \equiv 1 \, mod \, p^\alpha \equiv 1 \, mod \, q^\beta \equiv 1 \, mod \, r^\gamma$ etc. Hieraus und aus §. 135, XV. folgt aber

$$A^\varphi \equiv 1 \, mod \, (p^\alpha q^\beta r^\gamma \ldots) \text{ oder } \equiv 1 \, mod \, P$$

So hat man z. B. für $A = 15$, $P = 8 = 2^3$, da nun $m = (2-1)\,2^{3-1} = 1 \,.\, 2^2 = 4$ ist, $15^4 \equiv 1 \, mod \, 8$, oder es ist $15^4 - 1 = 50624$ durch 8 theilbar.

Ferner hat man für $A = 5$, $P = 24 = 2^3 \,.\, 3^1$, da nun $\varphi = (2-1)\,2^{3-1}(3-1)\,3^{1-1} = 1 \,.\, 2^2 \,.\, 2 \,.\, 3^0 = 8$ ist, $5^8 \equiv 1 \, mod \, 24$, oder es ist $5^8 - 1 = 390624$ durch 24 theilbar.

§. 141. ***Anwendung des verallgemeinerten Fermatschen Lehrsatzes auf die Lösung der unbestimmten Gleichungen vom ersten Grade.***

Nachdem Libri und Binet den Fermatschen Lehrsatz, in welchem p als Primzahl vorausgesetzt wird, zur Auflösung der

unbestimmten Gleichungen vom ersten Grade in speziellen Fällen benutzt hatten, hat Cauchy *(Exercices d'Analyse et de Physique mathématique)* die vorstehende Erweiterung des Fermatschen Lehrsatzes zur allgemeinen Auflösung jener Gleichungen in Anwendung gebracht. Das Prinzip ist folgendes.

Die Lösung der Gleichung $ax - py = c$ kann bekanntlich von der Lösung der Gleichung

(1) $$ax - py = 1$$

abhängig gemacht werden, worin a und p kein gemeinschaftliches Maass enthalten dürfen. Um die allgemeine Auflösung der letzteren Gleichung darzustellen, braucht man nur irgend eine spezielle, welche wir mit x_1, y_1 bezeichnen wollen, gefunden zu haben. Das Letztere kann sofort nach dem verallgemeinerten Fermatschen Lehrsatze geschehen, indem man aus den (stets positiv zu nehmenden) Primfaktoren der Zahl p die Grösse φ bestimmt und beachtet, dass $a^{\varphi} \equiv 1 \; mod\, p$, also $a^{\varphi} - 1 = vp$ oder

(2) $$a \,.\, a^{\varphi-1} - pv = 1$$

ist. Hiernach hat man unmittelbar als spezielle Auflösung der Gl. (1)

(3) $$x_1 = a^{\varphi-1}, \quad y_1 = \frac{a^{\varphi} - 1}{p}$$

Eine spezielle Auflösung der Gleichung

(4) $$ax - py = c$$

erhält man, wenn man Gl. (2) mit c multiplizirt, wodurch dieselbe

(5) $$a \,.\, ca^{\varphi-1} - pv = c$$

wird, und nun

(6) $$x_1 = ca^{\varphi-1}, \quad y_1 = \frac{c\,(a^{\varphi} - 1)}{p}$$

setzt.

Die allgemeine Auflösung ist immer

(7) $$x = x_1 + pw, \quad y = y_1 + aw$$

worin w eine willkürliche ganze Zahl bezeichnet.

Beispiel 1. In §. 29 war gegeben: $25x + 13y = 37$. Hier ist $p = -13$, also $\varphi = 13 - 1 = 12$, folglich

$$x = 37 \,.\, 25^{11} - 13w, \quad y = -\frac{37(25^{12} - 1)}{13} + 25w$$

Beispiel 2. In §. 26 war ferner gegeben: $23x - 15y = 30$. Hier ist $p = 15 = 3 \,.\, 5$, also $\varphi = (3 - 1)(5 - 1) = 8$, folglich

$$x = 30 \,.\, 23^{7} + 15w, \quad y = \frac{30(23^{8} - 1)}{15} + 23w$$

Beispiel 3. Es sei $35x - 18y = -10$. Hier ist $p = 18 = 2 \,.\, 3^2$, also $\varphi = (2-1)(3-1)3^{2-1} = 6$, folglich

$$x = -10 \,.\, 35^5 + 18w, \quad y = \frac{-10(35^6 - 1)}{18} + 35w$$

Beispiel 4. Es sei $5x - 2y = 1$. Hier ist $p = 2$, also $\varphi = 2 - 1 = 1$, folglich

$$x = 1 \,.\, 5^0 + 2w = 1 + 2w$$

$$x = \frac{1(5^1 - 1)}{2} + 5w = 2 + 5w$$

Wir haben jetzt fünf verschiedene Methoden zur Auflösung der unbestimmten Gleichungen vom ersten Grade mit zwei Unbekannten mitgetheilt. Die erste in §. 28, welche von Euler herrührt, die zweite in §. 30, welche in ihren Grundzügen von Bachet angegeben ist, die dritte, welche wir in §. 114 aus der Auflösung der quadratischen Gleichungen abstrahirt haben, die vierte in §. 137, welche wir auf die Reste der Vielfachen einer Zahl gestützt haben, und die fünfte, soeben vorgetragene, welche Cauchy aus den Eigenschaften der Reste der Potenzen einer Zahl abgeleitet hat.

Obgleich die letztere Methode in den meisten Fällen wegen der zu berechnenden hohen Potenzen etwas mühsam werden kann; so ist sie doch sehr beachtenswerth, weil nach ihr, wenn die Primfaktoren des Koeffizienten von x oder y bekannt sind, die Auflösung einer unbestimmten Gleichung vom ersten Grade in allgemeinen Zeichen dargestellt werden kann.

§. 142. *Die Reste der sukzessiven Potenzen einer gegebenen Zahl.*

I. Der Fermatsche Lehrsatz spricht eine wichtige Beziehung zwischen der Potenz der Zahl a vom Grade $p-1$ und der in a nicht enthaltenen Primzahl p aus. Es ist jedoch von Interesse, die Beziehungen zwischen p und den übrigen Potenzen von a näher zu untersuchen.

Denken wir uns zu dem Ende die kleinsten positiven Reste der sukzessiven Potenzen a^0, a^1, a^2, a^3... gebildet. Offenbar wird, nachdem der Rest irgend einer Potenz a^n erzeugt ist, der Rest der nächstfolgenden Potenz a^{n+1} erhalten, wenn man a^n mit a multiplizirt und das Produkt durch p dividirt, oder einfacher, wenn man den Rest von a^n mit dem Reste von a multiplizirt und dieses Produkt durch p dividirt. Hieraus erhellet, dass jeder folgende Rest durch den nächst vorhergehenden bedingt ist. Die Reste werden also, da sie sämmtlich $< p$ sind, von einer gewissen Stelle an Perioden bilden. Es setzt aber auch jeder spätere Rest mit Nothwendigkeit den einzigen unmittelbar vorhergehenden Rest voraus, sodass nie-

mals zwei verschiedene Reste Ein und denselben nächst folgenden hervorbringen können. Denn sonst müsste für zwei verschiedene Zahlen r' und r'', welche beide $<p$ sind, $ar' \equiv ar''$, also auch, da a und p relativ prim sind, $r' \equiv r''$ sein, was einen Widerspruch enthält. Hieraus folgt, dass die Periode der fraglichen Reste schon mit dem von $a^0 = 1$, also mit dem obersten Reste 1 beginnen muss.

Dasselbe bestätigt sich durch folgende Betrachtung. Nehmen wir die obersten Kongruenzen aus §. 136 für die sukzessiven Vielfachen von a, mit Ausschluss der ersten $0 . a \equiv 0$, vor Augen, und zwar folgende $p - 1$ Kongruenzen:

(A)

$$\begin{gathered} 1a \equiv r_1 \\ 2a \equiv r_2 \\ 3a \equiv r_3 \\ \vdots \\ (p-1)a \equiv r_{p-1} \end{gathered}$$

Hierin kommen alle Zahlen $1, 2, 3 \ldots (p-1)$ sowol als Faktoren der Zahlen a, wie auch als Reste r vor. Nehmen wir nun aus dieser Reihe eine gewisse Gruppe von Kongruenzen heraus, die in folgender Beziehung zu einander stehen. Zuvörderst die oberste mit dem Faktor 1, also $1a \equiv r_1$. Alsdann immer diejenige, in welcher der Faktor von a gleich dem Reste aus der unmittelbar vorher notirten Kongruenz ist. Diese Kongruenzen wollen wir so bezeichnen:

(B)

$$\begin{gathered} 1a \equiv R_1 \\ R_1 a \equiv R_2 \\ R_2 a \equiv R_3 \\ R_3 a \equiv R_4 \\ \vdots \\ R_{m-3} a \equiv R_{m-2} \\ R_{m-2} a \equiv R_{m-1} \\ R_{m-1} a \equiv 1 \end{gathered}$$

Es ist klar, dass sich endlich einmal eine schon notirte Kongruenz K_s bei K_t wiederholen muss. Alsdann müssen sich aber, weil man nach dem vorstehenden Gesetze immer nur aus einer einzigen der gegebenen Kongruenzen (A) in die nächst folgende der neuen Gruppe (B) gelangen kann, alle der Kongruenz K_s vorhergehenden Kongruenzen wiederholt haben. Es muss also zunächst die oberste Kongruenz $1a \equiv R_1$ wiederkehren. Die dieser Kongruenz unmittelbar vorhergehende Kongruenz der neuen Gruppe, welche den Rest 1 besitzt, sei $R_{m-1}\, a \equiv 1$. Mit dieser Kongruenz beschliessen wir die

Gruppe (B), welche m Kongruenzen enthält. Die m Reste $1, R_1, R_2 \ldots R_{m-1}$ sind nun sämmtlich verschieden und $< p$. Der Rest R_1 ist $= r_1$ und der Rest 1 kann systematisch mit R_m bezeichnet werden.

Substituirt man vermöge §. 135, XI. in die zweite Kongruenz der Gruppe (B) für R_1 den Werth a, welcher wegen der ersten Kongruenz zu R_1 kongruent ist; so kommt $a^2 \equiv R_2$. Substituirt man dann in die dritte Kongruenz für R_2 den Werth a^2, welcher wegen der eben gefundenen Kongruenz zu R_2 kongruent ist; so kommt $a^3 \equiv R_3$ u. s. f. Dies gibt die Gruppe

(C)

$$\begin{aligned} a &\equiv R_1 \\ a^2 &\equiv R_2 \\ a^3 &\equiv R_3 \\ &\vdots \\ a^{m-1} &\equiv R_{m-1} \\ a^m &\equiv 1 \end{aligned}$$

Hieraus erkennt man, dass die Reste der Potenzen $a, a^2, a^3 \ldots a^m$ sämmtlich verschieden sind, dass also ausser $a^0 = 1$, a^m die niedrigste Potenz von a ist, welche den Rest 1 besitzt. Die Periode der Reste der Potenzen von a hat also m Glieder.

Wenn durch die vorhin aus den Kongruenzen (A) ausgewählte Gruppe (B) von m Kongruenzen sämmtliche $p - 1$ gegebene Kongruenzen erschöpft sind, also $m = p - 1$ ist; so hat man $a^m = a^{p-1} \equiv 1$, also den Fermatschen Lehrsatz.

II. Wenn aber hierdurch jene $p - 1$ Kongruenzen nicht erschöpft sind, also $m < p - 1$ ist; so kann man eine der (B) ähnliche Gruppe von Kongruenzen aus den gegebenen (A) auswählen, indem man mit einer beliebigen Kongruenz beginnt, welche unter den obigen m der Gruppe (B) noch nicht enthalten ist. Diese Kongruenz sei durch $R'_n a \equiv R'_1$ bezeichnet. Als zweite, dritte, vierte etc. Kongruenz werde immer diejenige genommen, in welcher der Faktor von a gleich dem Reste in der vorhergehenden ist. Die neue Gruppe sei demnach

(B')

$$\begin{aligned} R'_n a &\equiv R'_1 \\ R'_1 a &\equiv R'_2 \\ R'_2 a &\equiv R'_3 \\ &\vdots \\ R'_{n-3} a &\equiv R'_{n-2} \\ R'_{n-2} a &\equiv R'_{n-1} \\ R'_{n-1} a &\equiv R'_n \end{aligned}$$

Aus dem schon oben angeführten Grunde muss zunächst

die erste Kongruenz wiederkehren. Dieser vorher geht eine Kongruenz von der Form $R'_{n-1} \equiv R'_n$, mit welcher wir die neue Gruppe (B′) schliessen. Die Zahl der Kongruenzen in (B′) sei n.

Es ist klar, dass unter diesen n Kongruenzen keine der in der Gruppe (B) enthaltenen m Kongruenzen vorkommen kann, weil sonst alle übrigen, und demnach auch die erste darin vorkommen müsste, was der Voraussetzung widerspricht. Demnach sind die n Reste R'_1, R'_2, $\ldots R'_{n-1}$, R'_n nicht allein unter sich, sondern auch von den m Resten R_1, $R_2 \ldots R_{m-1}$, 1 verschieden.

Substituiren wir nun wie früher in die zweite Kongruenz für R'_1 den ihm nach der ersten Kongruenz kongruenten Werth $R'_n a$; so ergibt sich $R'_n a^2 \equiv R'_2$. Substituiren wir dann in die dritte für R'_2 den ihm nach der eben gefundenen Kongruenz kongruenten Werth $R'_n a^2$; so kommt $R'_n a^3 \equiv R'_3$ u. s. f. Dies gibt eine der (C) ähnliche Gruppe:

(C′)

$$R'_n a \equiv R'_1$$
$$R'_n a^2 \equiv R'_2$$
$$R'_n a^3 \equiv R'_3$$
$$\vdots$$
$$R'_n a^{n-1} \equiv R'_{n-1}$$
$$R'_n a^n \equiv R'_n$$

Dividirt man die letzte Kongruenz durch die Zahl R'_n, welche $< p$, also da p eine Primzahl, auch relativ prim zu p ist; so erhält man $a^n \equiv 1$. Wir haben also eine zweite Potenz von a gefunden, welche den Rest 1 besitzt, und können ebenfalls behaupten, dass sie ausser $a^0 \equiv 1$ die niedrigste sei, welche den Rest 1 hat. Denn wäre für $s < n$ auch $a^s \equiv 1$; so hätte man durch Multiplikation mit R'_n $R'_n a^s \equiv R'_n$. Nach der betreffenden Kongruenz aus der Gruppe (C′) ist aber $R'_n a^s \equiv R'_s$. Es müsste also $R'_s \equiv R'_n$ folglich $R'_s = R'_n$, mithin $s = n$ sein.

Da nun sowol a^n, wie a^m ausser a^0 die niedrigste Potenz von a mit dem Reste 1 ist; so muss $n = m$ sein; es müssen also die beiden Gruppen (B) und (C) gleich viel Kongruenzen enthalten.

Wären nun auch durch die jetzt betrachteten $m + n = 2m$ Kongruenzen der beiden Gruppen (B) und (B′) die ursprünglich gegebenen $p - 1$ Kongruenzen der Gruppe (A) noch nicht erschöpft; so könnte man aus den übrig gebliebenen eine dritte, vierte etc. Gruppe nach demselben Gesetze ausscheiden. Da jede dieser Gruppen m Kongruenzen enthält, und endlich alle $p - 1$ gegebenen vollständig erschöpft werden müssen, so folgt, dass wenn nicht $m = p - 1$ ist, m ein Faktor von $p - 1$ sein

wird. Aber auch in diesem Falle, wo $p-1=mn$ sein möge, folgt aus $a^m \equiv 1$ der Fermatsche Lehrsatz $a^{mn} = a^{p-1} \equiv 1$.

III. Die vorstehende Untersuchung lehrt nicht bloss, dass der Rest 1 schon bei einer niedrigeren Potenz, als die $(p-1)$ste von a wiederkehren kann, sondern sie gibt auch ein einfaches Mittel an die Hand, die Reste der sukzessiven Potenzen von a darzustellen. Diese Rechnung würde nach dem im Eingange dieses Paragraphen beschriebenen Verfahren, wonach jeder vorhergehende Rest erst mit dem Reste von a zu multiplizieren und dann durch p zu dividiren ist, bei grossen Werthen von a und p leicht mühsam werden. Die Beziehung zwischen den Gruppen (C), (B), (A) lehrt dagegen, dass man die Reste R_1, $R_2 \ldots R_{m-1}$, 1 der Potenzen a, $a^2 \ldots a^{m-1}$, a^m mit Leichtigkeit aus der Gruppe (A) für die Reste der Vielfachen von a entnehmen kann.

So hat man z. B. für $a=15$, $p=11$, wenn man die Gruppe (B) aus den für dieses Beispiel schon in §. 136 angegebenen Kongruenzen für die Vielfachen von 15 entnimmt,

(B)	(C)
	$15^0 \equiv 1$
$1.15 \equiv 4$	$15^1 \equiv 4$
$4.15 \equiv 5$	$15^2 \equiv 5$
$5.15 \equiv 9$	$15^3 \equiv 9$
$9.15 \equiv 3$	$15^4 \equiv 2$
$3.15 \equiv 1$	$15^5 \equiv 1$

Die Periode der Reste der sukzessiven Potenzen von 15 hat also für den Model 11 nur 5 Glieder, und in der That ist 5 ein Faktor von $p-1=10$.

Für $a=17$, $p=11$ hat man

(A)	(B)	(C)
		$17^0 \equiv 1$
$1.17 \equiv 6$	$1.17 \equiv 6$	$17^1 \equiv 6$
$2.17 \equiv 1$	$6.17 \equiv 3$	$17^2 \equiv 3$
$3.17 \equiv 7$	$3.17 \equiv 7$	$17^3 \equiv 7$
$4.17 \equiv 2$	$7.17 \equiv 9$	$17^4 \equiv 9$
$5.17 \equiv 8$	$9.17 \equiv 10$	$17^5 \equiv 10$
$6.17 \equiv 3$	$10.17 \equiv 5$	$17^6 \equiv 5$
$7.17 \equiv 9$	$5.17 \equiv 8$	$17^7 \equiv 8$
$8.17 \equiv 4$	$8.17 \equiv 4$	$17^8 \equiv 4$
$9.17 \equiv 10$	$4.17 \equiv 2$	$17^9 \equiv 2$
$10.17 \equiv 5$	$2.17 \equiv 1$	$17^{10} \equiv 1$

Die Periode hat also hier $10 = p-1$ Glieder.

Wir bemerken noch, dass wenn $a \equiv 1$ ist, die Periode der Reste der Potenzen von a nur das Eine Glied 1 besitzt,

indem dann jede Potenz $a^n \equiv 1$ ist. Dies muss sich offenbar für jeden Werth von a ereignen, wenn der Model $p = 2$ ist.

Wenn $a \equiv p - 1$, oder auch bei Zulassung der kleinsten negativen Reste $a \equiv -1$ ist; so findet man leicht die zweigliederige Periode

$$\begin{array}{lll} a^0 \equiv 1 & \text{oder auch} & \equiv 1 \\ a^1 \equiv p - 1 & & \equiv -1 \\ a^2 \equiv 1 & & \equiv 1 \\ a^3 \equiv p - 1 & & \equiv -1 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \end{array}$$

sodass alsdann jede paare Potenz von a den kleinsten positiven Rest 1 und jede unpaare Potenz den kleinsten positiven Rest $p - 1$ oder den kleinsten negativen Rest -1 hat.

IV. Was die Verallgemeinerung der obigen Gesetze für den Fall betrifft, dass der Model p keine Primzahl ist; so hat man Folgendes zu beachten.

Wenn p keine Primzahl, aber relativ prim zu a ist; so wird die Gruppe (A) nach §. 136 unter den Resten $r_1, r_2 \ldots r_{p-1}$ sämmtliche Zahlen $1, 2 \ldots p - 1$ enthalten. Man kann also jedenfalls daraus die Gruppe (B) ausheben, deren erste Kongruenz $1a \equiv r$, und deren letzte Kongruenz $R_{m-1}a \equiv 1$ ist. Aus der Gruppe (B) folgt auch die Gruppe (C). Man kann also auch für diesen Fall nach der vorhin beschriebenen Methode die erste Periode der Reste der sukzessiven Potenzen von a bestimmen, und dieselbe wird stets zu einer Potenz a^m führen, welche den Rest 1 besitzt und ausser a^0 die niedrigste ist. Allein man kann nicht behaupten, dass m ein Faktor von $p - 1$ sei. Denn wenn man die Gruppe (B') und daraus die Gruppe (C') bildet; so lässt sich, weil p keine Primzahl ist, nicht allgemein behaupten, dass R'_n relativ prim zu p sei. Demnach kann man nicht allgemein die letzte Kongruenz von (C') durch R'_n dividiren, also auch nicht den Schluss $a^n \equiv 1$ machen. Mithin liegt keine Nothwendigkeit vor, dass die Gruppe (C') und die übrigen ähnlich gebildeten ebenfalls m Kongruenzen enthalten, wie die erste (C). In diesem Falle ist also auch nicht allgemein nach dem Fermatschen Lehrsatze $a^{p-1} \equiv 1$. Aus §. 140 folgt vielmehr, dass der Exponent m der niedrigsten Potenz von a, welche $\equiv 1$ ist, sobald man den Model in der Form $p^\alpha q^\beta r^\gamma \ldots$ darstellt, ein Faktor der Zahl $(p-1)p^{\alpha-1}(q-1)q^{\beta-1}(r-1)r^{\gamma-1} \ldots$ ist.

So hat man z. B. für $a = 15$, $p = 8$

(A)	(B)	(C)
		$15^0 \equiv 1$
$1 . 15 \equiv 7$	$1 . 15 \equiv 7$	$15^1 \equiv 7$
$2 . 15 \equiv 6$	$7 . 15 \equiv 1$	$15^2 \equiv 1$
$3 . 15 \equiv 5$		
$4 . 15 \equiv 4$		
$5 . 15 \equiv 3$		
$6 . 15 \equiv 2$		
$7 . 15 \equiv 1$		

Die Periode der Reste der Potenzen von 15 für den Model $8 = 2^3$ hat also 2 Glieder, und es ist 2 nach dem verallgemeinerten Fermatschen Lehrsatze ein Faktor von $(2-1)2^{3-1} = 4$.

Wenn p mit a ein gemeinschaftliches Maass besitzt, gleichviel, ob p eine Primzahl ist oder nicht; so hat man in §. 136 gesehen, dass kein Vielfaches von a den Rest 1 haben kann. Demnach gibt es für diesen Fall auch keine Potenz von a, welche den Rest 1 zu besitzen vermag, was auch schon in §. 140 angemerkt ist.

§. 143. *Fernerweite Gesetze der Reste der sukzessiven Potenzen einer Zahl, und deren Beziehung zu den periodischen Dezimalbrüchen.*

I. Denken wir uns unter der Voraussetzung, dass a und p irgend zwei relativ prime Zahlen seien, für die Gruppe (B) der m Kongruenzen des vorhergehenden Paragraphen, worin R_1, $R_2 \ldots R_m$ die Reste der sukzessiven Potenzen von a nach dem Model p darstellen, und m den Exponenten der niedrigsten Potenz a^m bezeichnet, welche $\equiv 1 \; mod \, p$ ist, die gleichbedeutenden Gleichungen

(D) (E)

$$1a = v_0 p + R_1 \text{ woraus auch } \frac{a}{p} = v_0 + \frac{R_1}{p} \text{ folgt}$$

$$R_1 a = v_1 p + R_2 \qquad \frac{R_1}{p} = \frac{v_1}{a} + \frac{R_2}{ap}$$

$$R_2 a = v_2 p + R_3 \qquad \frac{R_2}{p} = \frac{v_2}{a} + \frac{R_3}{ap}$$

$$\vdots \qquad \qquad \vdots$$

$$R_{m-2} a = v_{m-1} p + R_{m-1}$$

$$R_{m-1} a = v_m p + R_m$$

an die Stelle gesetzt; so ergeben sich die Quotienten v_0, $v_1 \ldots$ und die Reste R_1, $R_2 \ldots$, indem man erst mit p in a dividirt und hierdurch den Quotienten v_0 nebst dem Reste R_1 bestimmt, alsdann R_1 mit a multiplizirt, mit p in das Produkt $R_1 a$ dividirt und dadurch den Quotienten v_1 nebst dem Reste R_2 be-

stimmt, alsdann R_2 mit a multiplizirt, mit p in das Produkt $R_2 a$ dividirt und dadurch den Quotienten v_2 nebst dem Reste R_3 bestimmt u. s. f. Sobald man durch dieses Verfahren zum ersten Male auf den Rest 1 stösst, ist derselbe für R_m zu nehmen, und die m Glieder der Gruppe (B), (C) oder (D) sind erschöpft. Im Übrigen gestattet dieses Verfahren eine Fortsetzung ins Unendliche, in Folge deren eine unendliche Wiederkehr derselben m periodischen Glieder eintritt.

So hat man z. B. für $a = 15$, $p = 11$

$11 \mid 15 \mid 1 = v_0$	$1 . 15 = 1 . 11 + 4$	$15^1 \equiv 4 \; mod \; 11$
$ 11$	$4 \; 15 = 5 . 11 + 5$	$15^2 \equiv 5$
$ 4 = R_1$	$5 . 15 = 6 . 11 + 9$	$15^3 \equiv 9$
$R_1 a = 60 \mid 5 = v_1$	$9 . 15 = 12 . 11 + 3$	$15^4 \equiv 3$
55	$3 . 15 = 4 . 11 + 1$	$15^5 \equiv 1$
$5 = R_2$	$\vdots$	$\vdots$
$R_2 a = 75 \mid 6 = v_2$		
66		
$9 = R_3$		
$R_3 a = 135 \mid 12 = v_3$		
132		
$3 = R_4$		
$R_4 a = 45 \mid 4 = v_4$		
44		
$1 = R_5 = R_m$		

Substituirt man bei unendlich gedachter Fortsetzung dieses Verfahrens in den Ausdruck von $\frac{a}{p}$ aus der ersten Gleichung der Gruppe (E) zuvörderst den Werth von $\frac{R_1}{p}$ aus der zweiten, dann den Werth von $\frac{R_2}{p}$ aus der dritten, dann den Werth von $\frac{R_3}{p}$ aus der vierten Gleichung u. s. f.; so kommt

$$(1) \quad \frac{a}{p} = v_0 + \frac{v_1}{a} + \frac{v_2}{a^2} + \frac{v_3}{a^3} + \ldots + \frac{v_{m-1}}{a^{m-1}} + \frac{v_0}{a^m} + \frac{v_1}{a^{m+1}} + \text{etc.}$$

Dies ist eine unendliche und offenbar konvergirende Reihe für $\frac{a}{p}$. Die Nenner der einzelnen Glieder sind die sukzessiven Potenzen von a; die Zähler $v_0, v_1, v_2 \ldots v_{m-1}, v_0, v_1 \ldots$ sind die bei der obigen Rechnung entstehenden Quotienten der

einzelnen Divisionen, welche eine Periode von m Gliedern bilden.

Setzt man den Werth der ersten Periode

$$v_0 + \frac{v_1}{a} + \frac{v_2}{a^2} + \ldots + \frac{v_{m-1}}{a^{m-1}} = \frac{v_0 a^{m-1} + v_1 a^{m-2} + v_2 a^{m-3} + \ldots + v_{m-1}}{a^{m-1}}$$
$$= \frac{V}{a^{m-1}}$$

also

(2) $$V = v_0 a^{m-1} + v_1 a^{m-2} + v_2 a^{m-3} + \ldots + v_{m-1}$$

so nimmt jene unendliche Reihe die Form

$$\frac{a}{p} = \frac{V}{a^{m-1}}\left(1 + \frac{1}{a^m} + \frac{1}{a^{2m}} + \frac{1}{a^{3m}} + \ldots\right)$$
$$= \frac{V}{a^{m-1}} \cdot \frac{a^m}{a^m - 1} = \frac{Va}{a^m - 1}$$

an, woraus

(3) $$a^m - 1 = Vp$$

also der Fermatsche Lehrsatz folgt. Zugleich ergibt sich hieraus die Beziehung

(4) $$V = \frac{a^m - 1}{p} = v_0 a^{m-1} + v_1 a^{m-2} + v_2 a^{m-3} + \ldots + v_{m-1}$$

Für das obige Beispiel $a = 15$, $p = 11$ hat man

$$\frac{15}{11} = 1 + \frac{5}{15} + \frac{6}{15^2} + \frac{12}{15^3} + \frac{4}{15^4} + \frac{1}{15^5} + \frac{5}{15^6} + \ldots$$

$$V = \frac{15^5 - 1}{11} = 1 \,.\, 15^4 + 5 \,.\, 15^3 + 6 \,.\, 15^2 + 12 \,.\, 15 + 4$$

Wenn der Model allgemein eine zusammengesetzte Zahl von der Form $p^\alpha q^\beta r^\gamma \ldots$ ist; so weiss man aus dem Früheren, dass die Gliederzahl m der vorstehenden Periode oder des Ausdruckes von V ein Faktor der Zahl $(p-1)p^{\alpha-1}(q-1)q^{\beta-1}(r-1)r^{\gamma-1}\ldots$ ist, welche sich auf $p-1$ reduzirt, wenn der Model eine Primzahl p ist.

II. Die vorstehenden Resultate führen zu einer Betrachtung über die periodischen Dezimalbrüche. Wenn nämlich $a = 10$ ist; so stellt die sub I. beschriebene Operation offenbar das gewöhnliche Divisionsverfahren dar, mittelst dessen der Bruch $\frac{10}{p}$ in einen Dezimalbruch verwandelt wird. Enthält nun der Nenner p keinen der Primfaktoren 2 und 5, ist derselbe also relativ prim zu 10, so sind v_0, v_1, $v_2 \ldots v_{m-1}$ die Ziffern der Periode des Dezimalbruches, welcher $= \frac{10}{p}$ ist, während R_1, $R_2 \ldots R_m$

die vor der Anhängung der sukzessiven Dezimalstellen entstehenden Reste sind, deren letzter nothwendig $=1$ werden muss.

So hat man z. B. für $p=7$, wenn man $\frac{10}{7}$ in einen Dezimalbruch verwandelt,

```
7|10|1,42857...      10¹ ≡ 3
   7                 10² ≡ 2
  ──                 10³ ≡ 6
   30                10⁴ ≡ 4
   28                10⁵ ≡ 5
   ──                10⁶ ≡ 1
    20
    14
    ──
     60
     56
     ──
      40
      35
      ──
       50
       49
       ──
        1
```

Die Gliederzahl der Periode eines solchen Dezimalbruches ist also $=m$. Man kann demnach aus dieser Gliederzahl auf die niedrigste Potenz von 10 schliessen, welche $\equiv 1 \bmod p$ ist. Umgekehrt folgt, dass diese Gliederzahl ein Faktor von $p-1$ sei, insofern der Nenner p eine Primzahl ist, oder ein Faktor von $(p-1)p^{\alpha-1}(q-1)q^{\beta-1}\ldots$, insofern der Nenner $=p^{\alpha}q^{\beta}\ldots$ ist. So hat im obigen Beispiele die Periode des Bruches $\frac{10}{7}$ überhaupt $6=7-1$ Glieder.

Die letzteren Sätze gelten offenbar auch dann, wenn der in einen Dezimalbruch verwandelte Bruch $=\frac{a}{p}$ ist, dessen Zähler einen ganz beliebigen, zu p relativ primen Werth hat. In diesem allgemeineren Falle setze man $a=vp+R'_m\equiv R'_m$, sodass v_0 die grössten, in dem Bruche $\frac{a}{p}$ enthaltenen Ganzen bezeichne. Bei der ferneren Rechnung entstehen nun die Gleichungen

$$R'_m a = v_0 p + R'_1, \quad R'_1 a = v_1 p + R'_2, \quad R'_2 a = v_2 p + R'_3 \text{ etc.}$$

welche den Kongruenzen der Gruppe (B′) des vorhergehenden Paragraphen entsprechen und ebenfalls eine Periode von m Gliedern enthalten müssen, welche jedoch nicht, wie vorhin schon mit der ersten Ziffer, sondern allgemein mit der ersten auf die Ganzen v folgenden Ziffer des Dezimalbruches beginnt, auch den Rest 1 nicht enthält.

Hieraus folgt ferner, dass wenn p und a relativ prim sind, die Entwickelung von $\frac{a}{p}$ in einen Dezimalbruch immer eine Periode von derselben Länge enthält, welche nur vom Nenner p und nicht vom Zähler a abhängt.

Auch ist klar, dass die grösste Menge von periodischen Gliedern niemals $=p$, sondern höchstens $=p-1$ sein kann, wie im obigen Beispiele, wo man für $p=7$ eine Periode von 6 Gliedern erhielt.

Dass der Zähler a und der Nenner p eines in einen Dezimalbruch zu verwandelnden Bruches relativ prim seien, kann man offenbar stets voraussetzen. Enthielte aber der Nenner p beliebig viele Mal den Faktor 2 oder 5; so kann man *die*selben zum Verschwinden bringen, indem man den Zähler a mit einer genügend hohen Potenz von 10 multiplizirt, darauf den Bruch auf seine kleinste Benennung bringt und nach geschehener Dezimalentwickelung das Komma angemessen verrückt. Hieraus folgt, dass die Gesetze der entstehenden Periode hinsichtlich der Gliederzahl dieselben sind, welche der von den Faktoren 2 und 5 befreiete Nenner hervorbringen würde.

III. Denkt man sich statt irgend Einer der Gruppen (B), (B′), (B″)... von m Kongruenzen die entsprechende Gruppe (D), (D′), (D″)... von m Gleichungen gebildet und die letzteren addirt; so ergibt sich, wenn S die Summe aller m Reste und T die Summe aller m Quotienten bezeichnet,

$$Sa = Tp + S \quad \text{also}$$

(5) $$S(a-1) = Tp$$

Dass a und p relativ prim seien, wird immer vorausgesetzt: sind aber auch $a-1$ und p relativ prim; so muss offenbar die Summe T der Quotienten durch $a-1$ theilbar sein.

Da bei der Entwickelung eines Dezimalbruches für a nur der Werth 10 in Betracht kommt, also $a-1=9$ ist; so folgt, dass wenn der Nenner p des entwickelten Bruches nicht den Faktor 3 enthält, die Summe T der periodischen Ziffern stets durch 9 theilbar sein müsse. So ist z. B. im obigen Beispiele, wo $p=7$ war, $T=27$ in der That durch 9 theilbar.

Ist allgemein b das grösste gemeinschaftliche Maass von $a-1$ und p; so muss T durch $\frac{a-1}{b}$ theilbar sein.

Enthält also der Nenner des in einen Dezimalbruch entwickelten Bruches den Faktor 3, nicht aber den Faktor 9; so muss die Summe der periodischen Ziffern nothwendig durch 3 theilbar sein.

Ferner erhellet, dass im ersteren Falle, wo $a-1$ und p relativ prim sind, die Summe S der Reste durch p, im letzteren Falle jedoch, wo $a-1$ und p das grösste gemeinschaftliche Maass b haben, durch $\frac{p}{b}$ theilbar sei.

Enthält also der Nenner p des in einen Dezimalbruch verwandelten Bruches nicht den Faktor 3; so muss die Summe der den periodischen Quotienten entsprechenden Reste durch p theilbar sein. Enthält jedoch jener Nenner den Faktor 3, nicht aber den Faktor 9; so muss diese Summe durch $\frac{p}{3}$ theilbar sein. Enthält endlich jener Nenner eine höhere Potenz von 3, als die erste; so muss diese Summe durch $\frac{p}{9}$ theilbar sein. So ist z. B. im obigen Beispiele: wo $p=7$ war, $S=21$ durch 7 theilbar.

§. 144. Der Wilsonsche Lehrsatz.

I. Dieser zuerst von Wilson gegebene Satz lautet: Wenn p eine Primzahl ist; so ist das um 1 vermehrte Produkt aller Zahlen, welche kleiner als p sind, durch p theilbar. Man hat also die Gleichung

(1) $$[1.2.3.4\ldots(p-1)]+1=vp$$

oder auch die gleichbedeutende Kongruenz

(2) $$1.2.3.4\ldots(p-1)\equiv-1 \; mod p$$

Zum Beweise dieses Satzes nehmen wir aus der Gruppe (C) des §. 142 die erste und die vorletzte Kongruenz, also $a\equiv R_1$ und $a^{m-1}\equiv R_{m-1}$, und multipliziren sie mit einander. Hierdurch erhält man, da $a^m\equiv 1$ ist,

(3) $$R_1 R_{m-1}\equiv 1$$

R_1 und R_{m-1} sind also zwei Zahlen $<p$, deren Produkt $\equiv 1$ ist. Solche zwei Zahlen nennt man Gefährten (*socii*).

Zwei Gefährten sind, wenn man sich für die Zahl a beliebige Werthe, welche jedoch stets zu p prim sein müssen, gesetzt denkt, nur in zwei Fällen einander gleich. Nämlich dann, wenn $R_1=1$ und wenn $R_1=p-1$ ist. Denn bezeichnet man zwei gleiche Gefährten allgemein mit x; so muss $xx\equiv 1$ oder $x^2-1=(x-1)(x+1)\equiv 0$ sein. Dies ist offenbar nur möglich, entweder wenn der Faktor $x-1$, oder wenn der Faktor $x+1$ ein Vielfaches der Primzahl p, also entweder wenn $x-1\equiv 0$, folglich $x\equiv 1$, oder wenn $x+1\equiv 0$, folglich $x\equiv -1\equiv p-1$ ist. Im ersteren Falle muss daher der Rest von x, d. i. der Werth von R_1 gleich 1 und im letzteren gleich $p-1$ sein.

Von jedem anderen Reste R_1, welcher $<p$, also auch

relativ prim zu p ist, ist mithin der Gefährte R_{m-1}, wenn es sonst einen solchen gibt, verschieden. Dass es aber einen solchen stets gebe, leuchtet ein, wenn man sich für $a = R_1$ die Gruppe (C) gebildet denkt, worin die erste Kongruenz $a \equiv R_1$ und die vorletzte $a^{m-1} \equiv R_{m-1}$ ist.

Es kann auch keine Zahl R_1, welche $< p$ ist, ausser diesem Gefährten R_{m-1} einen anderen Gefährten haben. Denn wäre ein solcher zweiter $= R_n$; so wäre sowol $R_1 R_{m-1} \equiv 1$, wie auch $R_1 R_n \equiv 1$, also $R_1 R_{m-1} \equiv R_1 R_n$, mithin, da R_1 relativ prim zu p ist, $R_{m-1} \equiv R_n$. Die letztere Bedingung erfordert aber, da R_{m-1} und R_n beide $< p$ sind, die Gleichheit dieser beiden Grössen.

Von den Zahlen $2, 3, 4 \ldots (p-2)$ sind also nur je zwei die Gefährten von einander. Von 1 ist 1 und von $p-1$ ist $p-1$ der Gefährte. Demnach ist das Produkt aller nach (3) gebildeten Kongruenzen, worin R_1, R_{m-1} nach und nach die Werthe von je zwei der Zahlen $2, 3, 4 \ldots (p-2)$ erhalten,

$$2 . 3 . 4 \ldots (p-2) \equiv 1$$

und wenn man mit $1 . (p-1) \equiv -1$ multiplizirt,

$$1 . 2 . 3 . 4 \ldots (p-1) \equiv -1$$

was zu beweisen war.

II. Zur Vervollständigung des im Wilsonschen Lehrsatze liegenden Gesetzes dient der Satz, dass wenn p keine Primzahl ist, die Grösse $1 . 2 . 3 \ldots (p-1) + 1$ nicht durch p theilbar ist. Denn wäre $p = st$ und

$$1 . 2 . 3 \ldots (p-1) + 1 = vp = vst$$

so würde sowol s, wie t, da beide > 1 und $< p$ sind, unter den Zahlen $2, 3 \ldots (p-1)$ vorkommen. Da sich nun in der vorstehenden Gleichung die rechte Seite durch s dividiren lässt; so müsste Dies auch mit der linken möglich sein. Da aber auf der linken Seite das erste Glied durch s theilbar ist; so müsste es auch das zweite Glied sein, welches den Werth 1 hat. Dies ist offenbar unmöglich, und hieraus folgt, dass für einen zusammengesetzten Werth von p die vorstehende Gleichung nicht bestehen kann.

Der Wilsonsche Lehrsatz liefert also ein Kriterium für eine Primzahl.

III. Dieser Satz lässt sich für jede Primzahl $p > 2$, welche also unpaar ist, noch in eine andere bemerkenswerthe Form bringen. Beachtet man nämlich, dass $p-1 \equiv -1$, $p-2 \equiv -2$, $p-3 \equiv -3$ u. s. w. ist; so hat man

$$1 . 2 . 3 \ldots (p-3)(p-2)(p-1) \equiv \left[1 . 2 . 3 \ldots \frac{p-1}{2}\right] \times$$

$$\left[\left(-\frac{p-1}{2}\right) \ldots (-3)(-2)(-1)\right] \equiv (-1)^{\frac{p-1}{2}} \left(1 . 2 . 3 \ldots \frac{p-1}{2}\right)^2$$

Da nun dieser Ausdruck nach dem Wilsonschen Lehrsatze auch $\equiv -1$ ist; so ergibt sich, wenn man beiderseits mit $(-1)^{\frac{p-1}{2}}$ multiplizirt und beachtet, dass $p-1$ paar, also $(-1)^{p-1} = 1$ ist,

$$(3) \qquad \left(1 . 2 . 3 \ldots \frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}}$$

Hat also die Primzahl p die Form $4n+1$; so ist

$$\left(1 . 2 . 3 \ldots \frac{p-1}{2}\right)^2 \equiv -1$$

und hat sie die Form $4n+3$; so ist

$$\left(1 . 2 . 3 \ldots \frac{p-1}{2}\right)^2 \equiv 1$$

§. 145. *Verallgemeinerung der früheren Sätze für den Fall, dass der Model keine Primzahl ist.*

I. Wenn der Model p eine Primzahl > 2 ist; so sind alle natürlichen Zahlen $1, 2, 3 \ldots (p-1)$, welche $< p$ sind, relativ prim zu p und keine ist der anderen kongruent. Diese Zahlen, deren Menge $p-1$ stets paar ist, und von denen die Eine Hälfte $< \frac{p}{2}$, die andere Hälfte $> \frac{p}{2}$ ist, und von denen jede Zahl der ersteren Hälfte mit einer Zahl der letzteren Hälfte die Summe p ausmacht, haben sich bei den bisherigen Untersuchungen von grosser Wichtigkeit erwiesen.

Wenn nun der Model P keine Primzahl ist; so übernehmen in sehr vielen Fällen die zu P relativ primen Zahlen, welche $< P$ sind, die Rolle der eben genannten natürlichen Zahlen, indem die Menge jener relativ primen Zahlen an die Stelle der Menge $P-1$ dieser natürlichen Zahlen tritt.

Ist also der Model P von der Form

$$(1) \qquad P = p^{\alpha} q^{\beta} \ldots$$

worin p, q verschiedene Primzahlen darstellen, und mithin nach §. 138 Gl. (7) die Menge φ der zu P relativ primen Zahlen, welche $< P$ sind, einschliesslich der Zahl 1,

$$(2) \qquad \varphi = p^{\alpha-1}(p-1) q^{\alpha-1}(q-1) \ldots$$

so übernimmt, wenn es sich um die Menge der zum Model relativ primen Zahlen handelt, φ die Rolle der früheren Zahl $p-1$ und $\frac{\varphi}{2}$ die Rolle von $\frac{p-1}{2}$.

Die wichtigsten hieraus sich ergebenden Resultate werden wir ohne umständlichen Beweis anführen dürfen, indem das

Beweisverfahren dem früheren in dem analogen Falle ganz gleich ist.

II. Es sei A eine zum Model P relativ prime Zahl.

Zunächst denken wir uns wie in §. 136 die Produkte aus A und den sukzessiv aufsteigenden zu P relativ primen Zahlen gebildet und die Reste aller dieser Produkte genommen. Dies wird φ Kongruenzen ergeben, auf deren rechten Seiten alle zu P relativ primen Zahlen, wenn auch nicht in der natürlichen Reihenfolge, erscheinen werden. Wäre z. B. $A = 22$, $P = 15$; so hätte man

$$\begin{aligned} 1 \,.\, 22 &\equiv 7 \\ 2 \,.\, 22 &\equiv 14 \\ 4 \,.\, 22 &\equiv 13 \\ 7 \,.\, 22 &\equiv 4 \\ 8 \,.\, 22 &\equiv 11 \\ 11 \,.\, 22 &\equiv 2 \\ 13 \,.\, 22 &\equiv 1 \\ 14 \,.\, 22 &\equiv 8 \end{aligned}$$

Multiplizirt man alle diese φ Kongruenzen mit einander; so kann man beiderseits mit dem Produkte aller zu P relativ primen Zahlen dividiren. Dies gibt

(3) $$A^{\varphi} \equiv 1 \; mod\, P$$

worin der schon in §. 140 auf eine andere Weise erhaltene verallgemeinerte Fermatsche Lehrsatz besteht.

Da φ stets eine paare Zahl ist (wennicht $P = 2$); so erhellet, dass man nothwendig haben müsse

(4) $$A^{\frac{\varphi}{2}} \equiv \pm 1 \; mod\, P$$

III. Setzen wir die eben beschriebene Gruppe von Kongruenzen, deren linke Seiten die Produkte aus A und den zu A relativ primen Zahlen sind, an die Stelle der Gruppe (A) des §. 142; so ergeben sich daraus sofort die dortigen Gruppen (B) und (C) und die daraus gezogenen Konsequenzen.

Der nächste Schluss daraus ist, dass die Reste der sukzessiven Potenzen von A eine Periode von lauter verschiedenen Zahlen bilden, deren Gliederzahl m ein Faktor von φ ist und deren letzter Rest $= 1$ ist, sodass in

(5) $$A^{m} \equiv 1 \; mod\, P$$

A^m die niedrigste Potenz von A darstellt, welche kongruent 1 ist.

IV. Wie in §. 144, so lässt sich auch hier zeigen, dass je zwei der Reste, welche die Gruppe (C) bilden, Gefährten sind, oder dass ihr Produkt $\equiv 1$ ist, während auch hier nur 1 und $P - 1$ Gefährten von sich selbst sind.

Dies führt ohne Weiteres zu dem verallgemeinerten Wilsonschen Lehrsatze, welcher aussagt, dass das Produkt aller zu P relativ primen Zahlen $\equiv -1 \, mod P$ sei.

V. Bezeichnen wir, wie in §. 142, Gruppe (C), auch hier die Reste der sukzessiven Potenzen von A mit R_1, $R_2 \dots R_{m-1}, R_m$, wovon der letzte $R_m = 1$ ist; so sind offenbar die paarweise zusammengehörigen Gefährten, wenn m paar ist,

$$R_1 R_{m-1}, \; R_2 R_{m-2}, \; R_3 R_{m-3} \dots R_{\frac{m}{2}} R_{\frac{m}{2}}$$

und wenn m unpaar ist,

$$R_1 R_{m-1}, \; R_2 R_{m-2}, \; R_3 R_{m-3} \dots R_{\frac{m-1}{2}} R_{\frac{m+1}{2}}$$

In beiden Fällen sind alle mit R bezeichneten Reste unter sich verschieden, auch verschieden von $R_m = 1$. Da aber im ersteren Falle, wo m paar ist, die beiden letzten Gefährten $R_{\frac{m}{2}}$ einander gleich sind; so können sie nur $= P - 1$ sein. In diesem Falle ist also

$$(6) \qquad A^{\frac{m}{2}} \equiv -1 \, mod P$$

und zwar ist $\frac{m}{2}$ der Exponent der niedrigsten Potenz von A, welche kongruent -1 ist.

Im zweiten Falle dagegen, wo m unpaar ist, kommen keine zwei gleichen Gefährten vor; es kann also unter den Resten R auch nicht der Werth $P - 1$ vorkommen: mithin gibt es unter diesen Umständen überhaupt keine Potenz von A, welche $\equiv -1 \, mod P$ wäre.

VI. Da der Exponent m der niedrigsten Potenz von A, welche $\equiv 1$ ist, ein Faktor von φ ist; so hat man $\varphi = mn$. Die Zahl n stellt alsdann die Anzahl der Gruppen (B), (B'), (B'')... dar, in welche sich die Gruppe (A) nach dem in §. 142 beschriebenen Verfahren auflös't.

Mit Ausschluss des einzigen Falles, wo $P = 2$, ist φ immer paar, also auch Eine der beiden Zahlen m und n paar.

Wenn nun n oder die Anzahl der eben erwähnten Gruppen paar ist; so hat man $A^{\frac{\varphi}{2}} = (A^m)^{\frac{n}{2}}$, also da $A^m \equiv 1$ ist, $A^{\frac{\varphi}{2}} \equiv 1$.

Wenn dagegen n unpaar ist, in welchem Falle m paar sein muss, hat man $A^{\frac{\varphi}{2}} = \left(A^{\frac{m}{2}}\right)^n$ und da nun nach (6) $A^{\frac{m}{2}} \equiv -1$ ist, $A^{\frac{\varphi}{2}} \equiv -1$.

In allen Fällen kann man also setzen

(7) $$A^{\frac{\varphi}{2}} \equiv (-1)^n$$

wodurch die Formel (4) eine nähere Bestimmung findet.

VII. Das Produkt der ersten m Potenzen von A ist $A^{\frac{m(m+1)}{2}}$. Ist m unpaar; so hat man für dieses Produkt $(A^m)^{\frac{m+1}{2}} \equiv 1$. Ist dagegen m paar; so hat man dafür $\left(A^{\frac{m}{2}}\right)^{m+1} \equiv (-1)^{m+1} \equiv -1$. Allgemein ist also jenes Produkt $\equiv (-1)^{m+1}$.

Berücksichtigt man Dies und erhebt nun jede der m Kongruenzen der Gruppe (C), ebenso jede der Gruppe (C′), der Gruppe (C″) u. s. w. auf die $m$te Potenz, multiplizirt auch einmal alle m Kongruenzen jeder einzelnen dieser Gruppen mit einander; so ergeben sich folgende Beziehungen.

$$R_1^m \equiv R_2^m \equiv \ldots \equiv R_m^m \equiv (-1)^{m+1} R_1 R_2 \ldots R_m \equiv 1$$
$$R_1'^m \equiv R_2'^m \equiv \ldots \equiv R_m'^m \equiv (-1)^{m+1} R_1' R_2' \ldots R_m'$$
$$R_1''^m \equiv R_2''^m \equiv \ldots \equiv R_m''^m \equiv (-1)^{m+1} R_1'' R_2'' \ldots R_m''$$
etc.

Dies sind n Gruppen von Kongruenzen. Bezeichnet man den kleinsten Rest des Produktes aus $(-1)^{m+1}$ und den m Resten auf der rechten Seite der ersten, zweiten, dritten ... $n$ten Gruppe resp. mit $S_1, S_2 \ldots S_n$; so ergibt sich leicht

$$S_1^n \equiv S_2^n \equiv \ldots \equiv S_n^n \equiv 1$$

§. 146. *Allgemeine Sätze über die Kongruenzen höherer Grade.*

I. Eine Kongruenz höheren Grades, wie

(1) $$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n \equiv 0 \; mod\, p$$

verlangt, dass für x eine Zahl gesucht werde, wodurch die linke Seite ein Vielfaches von p wird.

Nach §. 135, XI. kann man annehmen, entweder dass sämmtliche Koeffizienten $a_0, a_1 \ldots a_n$ positiv und negativ und numerisch $\leqq \frac{p}{2}$, oder dass sie sämmtlich positiv und $< p$ seien, indem man für jeden seinen kleinsten numerischen oder seinen kleinsten positiven Rest nach dem Model p setzen kann. Auch braucht man nur diejenigen Auflösungen für x zu betrachten, welche positiv und negativ und numerisch $\leqq \frac{p}{2}$, oder welche positiv und $< p$ sind, da aus irgend Einer Auflösung dieser Art wie x' immer eine unendliche Reihe anderer von der Form $x = x' + wp$ folgt, welche sämmtlich dem Werthe x' nach dem Model p kongruent sind, sodass dann allgemeiner $x \equiv x' \; mod\, p$ ist.

Analog der Benennung bei den Gleichungen, heisst x eine Wurzel der Kongruenz (1).

II. Man kann behaupten, dass wenn der Model p eine in dem Koeffizienten a_0 der höchsten Potenz von x nicht aufgehende Primzahl ist, wobei also, wenn für alle Koeffizienten ihre kleinsten positiven Reste gesetzt sind, $a_0 > 0$ und $< p$ sein wird, die Kongruenz vom $n$ten Grade nicht mehr als n einander nicht kongruente Wurzeln, oder nicht mehr als n verschiedene positive Werthe von x, welche $< p$ sind, haben kann.

Denn es seien $x_1, x_2 \ldots x_m$ solche m verschiedene Werthe von x und $m > n$. Dividirt man mit $x - x_1$ in die linke Seite der gegebenen Kongruenz; so kommt man auf den Rest $a_0 x_1^n + a_1 x_1^{n-1} + a_2 x_1^{n-2} + \ldots + a_{n-1} x_1 + a_n$. Der Quotient ergibt sich in der Form $a_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} + \ldots + b_{n-2} x + b_{n-1}$, worin $b_1, b_2 \ldots b_{n-1}$ lauter ganze Zahlen sind. Man kann demnach statt der gegebenen Kongruenz schreiben

$$(x - x_1)(a_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} + \ldots + b_{n-2} x + b_{n-1})$$
$$+ (a_0 x_1^n + a_1 x_1^{n-1} + a_2 x_1^{n-2} + \ldots + a_{n-1} x_1 + a_n) \equiv 0$$

oder da das zweite Glied auf der linken Seite nach der Voraussetzung ein Vielfaches von p ist,

(2) $$(x - x_1)(a_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} + \ldots + b_{n-2} x + b_{n-1}) \equiv 0$$

Die vorstehende Kongruenz ist augenscheinlich für $x = x_1$ erfüllt, wie es auch die Voraussetzung fordert. Da dieselbe aber vorausgesetztermaassen ebenfalls für die übrigen $m - 1$ Werthe $x_2, x_3 \ldots x_m$ von x gelten soll, und alle diese Werthe verschieden unter einander und verschieden von x_1, auch $< p$ angenommen sind, mithin der Faktor $x - x_1$ für jeden dieser $m - 1$ Werthe von x einen absoluten Werth > 0 und $< p$, also einen zu p relativ primen Werth haben muss; so leuchtet ein, dass man für jeden der genannten $m - 1$ Werthe von x die Kongruenz (2) durch den Faktor $x - x_1$ dividiren kann, und dass mithin für diese $m - 1$ Werthe von x die Kongruenz

(3) $$a_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} + \ldots + b_{n-2} x + b_{n-1} \equiv 0$$

deren Grad um 1 geringer ist, als der der gegebenen, bestehen muss.

Behandelt man diese Kongruenz genau so wie die ursprüngliche, indem man nun mit $x - x_2$ dividirt; so gelangt man zu dem Schlusse, dass eine Kongruenz von der Form

(4) $$a_0 x^{n-2} + c_1 x^{n-3} + c_2 x^{n-4} + \ldots + c_{n-3} x + c_{n-2} \equiv 0$$

die $m - 2$ Wurzeln $x_3, x_4 \ldots x_m$ haben müsse.

Setzt man dieses Verfahren fort; so muss man nothwendig, wenn im Laufe der Rechnung, nach der Ausscheidung von t

Wurzeln, alle Glieder ausser dem höchsten verschwinden sollten, auf eine Kongruenz von der Form

(5) $$a_0 x^{n-t} \equiv 0$$

oder wenn sich dieser spezielle Fall nicht ereignet, nach der Ausscheidung von $n-1$ Wurzeln, auf eine Kongruenz von der Form

(6) $$a_0 x + q \equiv 0$$

stossen, in welcher letzteren auch $q = 0$ sein kann.

Im ersteren Falle (5) müsste, wenn man mit a_0 dividirt, die Kongruenz $x^{n-t} \equiv 0$ durch die $m-t$ Werthe $x_{t+1}, x_{t+2} \ldots x_m$ von x erfüllt werden. Diese Kongruenz kann aber offenbar keine anderen Auflösungen, als solche haben, welche Vielfache von p sind, welche also sämmtlich dem kleinsten Werthe $x = 0$ entsprechen. Es müsste also $x_{t+1} = x_{t+2} = \ldots = x_m = 0$ sein. Demnach kann die gegebene Kongruenz (1) nur die $t+1$ verschiedenen Auflösungen $x_1, x_2 \ldots x_t, x_{t+1}$ haben, worin $x_{t+1} = 0$ ist. Die Anzahl dieser Auflösungen ist aber durchaus kleiner als der Grad n jener Kongruenz.

Im letzteren Falle (6), wo man auf eine Kongruenz vom ersten Grade stösst, weiss man aus §. 137, dass eine solche Kongruenz nur eine einzige Wurzel $< p$ haben kann. Es müssten also alle Wurzeln $x_n, x_{n+1} \ldots x_m$, durch welche jene Kongruenz erfüllbar sein soll, einander gleich sein, also die Stelle einer einzigen x_n vertreten. Die gegebene Kongruenz (1) vom $n$ten Grade hätte also in diesem Falle genau n verschiedene Wurzeln, und nicht mehr.

III. Der obige Satz, dass eine Kongruenz vom $n$ten Grade höchstens n verschiedene positive Wurzeln $< p$ haben könne, ist also erwiesen. Aus der Entwickelung des Beweises abstrahirt man aber leicht noch folgende wichtige Beziehungen.

Wenn die gegebene Kongruenz (1) genau n verschiedene Wurzeln $x_1, x_2 \ldots x_n$ hat, wenn also $m = n$ ist; so lässt sie sich offenbar in die Form

(7) $$(x - x_1)(x - x_2)(x - x_3) \ldots (x - x_n) \equiv 0$$

bringen, indem man nach der Absonderung der ersten $n-1$ Faktoren an die Stelle der übrig bleibenden Kongruenz (6) vom ersten Grade die gleichbedeutende $x \equiv x_n$ oder $x - x_n \equiv 0$ setzt.

Wäre die Anzahl m der verschiedenen Wurzeln $< n$; so würde Das, was im obigen Satze bewiesen werden sollte, schon in der Voraussetzung liegen, und das vorstehende Beweisverfahren würde überflüssig sein. Stellt man dasselbe aber dennoch an; so kommt man zu dem Schlusse, dass die gegebene Kongruenz in die Form

(8) $$(x - x_1)(x - x_2) \ldots (x - x_m) \times \\ (a_0 x^{n-m} + q_1 x^{n-m-1} + q_2 x^{n-m-2} + \ldots + q_{n-m-1} x + q_{n-m}) \equiv 0$$

gebracht werden kann. Der polynomische Faktor oder vielmehr die daraus gebildete Kongruenz

(9) $a_0x^{n-m}+q_1x^{n-m-1}+q_2x^{n-m-2}+\ldots+q_{n-m-1}x+q_{n-m}\equiv 0$

hat nun entweder gar keine oder nur solche Wurzeln, welche unter den m verschiedenen Zahlen x_1, $x_2 \ldots x_m$ vorkommen. Denn wäre x_{m+1} eine von den letzteren verschiedene Wurzel der Kongruenz (9); so wäre dieser Werth offenbar auch eine Wurzel der gegebenen Kongruenz, weil dadurch die ganze linke Seite von (8) kongruent null werden würde. Die gegebene Gleichung hätte also nicht m, sondern $m+1$ verschiedene Wurzeln, was der Voraussetzung widerspricht.

Hätte aber die Kongruenz (9) irgend Eine der Zahlen x_1, $x_2 \ldots x_m$, z. B. x_1 zur Wurzel; so würde man auf der linken Seite von (9) den Faktor $x-x_1$ absondern können. Demnach hätte in der gegebenen Kongruenz (1) gleich von vorn herein der Faktor $x-x_1$ zweimal oder es hätte der quadratische Faktor $(x-x_1)^2$ abgesondert werden können. Nachdem unter diesen Umständen die Kongruenz (9) von dem Faktor $x-x_1$ befreiet ist, kann der sich ergebende Quotient vom Grade $n-m-1$ wieder in früherer Weise behandelt werden. Dieses Verfahren führt endlich zu dem Schlusse, dass die gegebene Kongruenz (1) stets auf die Form (8) gebracht werden kann, wenn man darin unter x_1, $x_2 \ldots x_m$ (nach Analogie der Gleichungen) die m gleichen und ungleichen Wurzeln derselben versteht. Ist der übrig bleibende polynomische Faktor, welcher die linke Seite der Kongruenz (9) bildet, vom ersten Grade; so muss genau $m=n$ sein, die gegebene Kongruenz vom $n$ten Grade muss also genau n gleiche und ungleiche Wurzeln haben und sich auf die noch einfachere Form (7) bringen lassen. Ist dagegen der fragliche Faktor von einem höheren, als dem ersten Grade, also $m<n$; so muss (9) eine unlösbare Kongruenz sein.

Der Fall, wo eine gewisse Anzahl, z. B. t Wurzeln $=0$ wären, macht von dem vorstehenden keine Ausnahme. Es müsste sich dann $(x-0)^t=x^t$ von der gegebenen Kongruenz absondern lassen, die letztere müsste also die Form

(10) $a_0x^n+a_1x^{n-1}+\ldots+a_{n-t}x^t\equiv 0$

haben.

IV. Wenn die gegebene Kongruenz (1) vom $n$ten Grade genau n gleiche und ungleiche Wurzeln hat, also auf die Form (7) gebracht werden kann, und man substituirt für den letzten Faktor $x-x_n$ den ihm kongruenten Werth a_0x+q oder auch was genau Dasselbe sein muss, den Werth $a_0x-a_0x_n\equiv a_0(x-x_n)$; so entspricht Dies einer Multiplikation der Kongruenz (7) mit dem Faktor a_0. Führt man hierauf alle auf der linken Seite

von (7) vorgeschriebenen Multiplikationen der Binome $x-x_1$, $x-x_2\ldots$ aus; so muss sich offenbar ein Ausdruck ergeben, in welchem die Koeffizienten der verschiedenen Potenzen von x den Koeffizienten der entsprechenden Potenzen von x in der Form (1) in Beziehung zum Model p kongruent sind. Dies gibt folgende Beziehungen zwischen den Koeffizienten einer Kongruenz $n$ten Grades und ihren Wurzeln, insofern nach der Voraussetzung die Anzahl dieser Wurzeln genau $=n$ ist.

$$(11)\quad \begin{cases} a_0(x_1+x_2+\ldots+x_n) \equiv -a_1 \equiv p-a_1 \\ a_0(x_1x_2+x_1x_3+x_2x_3+\ldots) \equiv a_2 \\ a_0(x_1x_2x_3+\ldots) \equiv -a_3 \equiv p-a_3 \\ a_0(x_1x_2x_3x_4+\ldots) \equiv a_4 \\ \quad\vdots \\ a_0x_1x_2x_3\ldots x_n \equiv (-1)^n a_n \end{cases}$$

V. Aus dem obigen Satze II. folgt, dass es unter den positiven Zahlen, welche $<p$ sind, also unter den p Zahlen $0, 1, 2\ldots p-1$, höchstens n geben kann, deren $n$te Potenzen einander kongruent sind, für welche man also

$$(12)\qquad x_1^n \equiv x_2^n \equiv x_3^n \equiv \ldots \equiv x_n^n$$

hat. Denn alle diese Werthe $x_1, x_2\ldots x_n$ erfüllen, wenn sie für x substituirt werden, die Kongruenz

$$(13)\qquad x^n \equiv x_1^n \text{ oder auch } x^n - x_1^n \equiv 0$$

Gäbe es nun mehr als n Zahlen $x_1, x_2, x_3\ldots$ von der Beschaffenheit (12); so müsste die Kongruenz (13) mehr als n Wurzeln haben, was unmöglich ist.

VI. Wenn, wie hier immer vorausgesetzt wird, der Model p eine Primzahl ist; so ist nach dem Fermatschen Lehrsatze (§. 139) für jeden der p Werthe $0, 1, 2, 3\ldots p-1$ für x

$$(14)\qquad x^{p-1} \equiv 1 \text{ oder } x^{p-1}-1 \equiv 0 \bmod p$$

Diese Kongruenz vom Grade $p-1$ hat also stets $p-1$ verschiedene Wurzeln, und man kann auch für dieselbe schreiben

$$(15)\qquad (x-1)(x-2)(x-3)\ldots(x-(p-1)) \equiv 0$$

Hieraus und aus dem Satze II. folgt auch, dass wenn man das Binom $x^{p-1}-1$ in zwei Polynome vom Grade m und n zerlegt, sodass $m+n=p-1$ und

$$(16)\qquad x^{p-1}-1 = (x^m+a_1x^{m-1}+\ldots+a_{m-1}x+a_m)\times (x^n+b_1x^{n-1}+\ldots+b_{n-1}x+b_n) \equiv 0$$

ist, die Kongruenz

$$(17)\qquad x^m+a_1x^{m-1}+\ldots+a_{m-1}x+a_m \equiv 0$$

genau m und die Kongruenz

$$(18)\qquad x^n+b_1x^{n-1}+\ldots+b_{n-1}x+b_n \equiv 0$$

genau n verschiedene Wurzeln hat, weil das Produkt aus Bei-

den genau $m+n=p-1$ Wurzeln besitzt und (17) nicht mehr als m, auch (18) nicht mehr als n Wurzeln haben kann.

Eine jede der beiden Kongruenzen (17) und (18) kann auch noch mit einem Koeffizienten wie a_0 und b_0 multiplizirt, also auf die Form der Kongruenz (1) gebracht werden.

Wir machen noch auf folgendes aus der Form der Kongruenz $x^{p-1}-1\equiv 0$ unmittelbar sich ergebendes Zahlengesetz aufmerksam: Bildet man die Summe S_1, S_2, $S_3 \ldots S_{p-1}$ der Produkte aus je Einer, je zwei, je drei... je $(p-1)$ der Zahlen 1, 2, 3...$(p-1)$, und beachtet, dass die letzteren Zahlen die Wurzeln der in Rede stehenden Kongruenz sind, ferner dass der erste und letzte Koeffizient dieser Kongruenz resp. $=1$ und -1 ist, während alle übrigen $=0$ sind; so hat man nach den obigen Kongruenzen (11), indem hier $n=p-1$ eine paare Zahl ist,

$$S_1 = 1+2+3+\ldots+(p-1)\equiv 0$$
$$S_2 = [1.2]+[1.3]+\ldots+[(p-2)(p-1)]\equiv 0$$
$$S_3 = [1.2.3]+\ldots+[(p-3)(p-2)(p-1)]\equiv 0$$
$$\vdots$$
$$S_{p-2} = [1.2.3\ldots(p-2)]+\ldots+[2.3.4\ldots(p-1)]\equiv 0$$
$$S_{p-1} = 1.2.3\ldots(p-1)\equiv -1$$

Die letzte dieser Kongruenzen stellt den Wilsonschen Lehrsatz dar, und die übrigen lehren, dass jede Summe S durch die Primzahl p theilbar sei. So hat man z. B. für die Primzahl $p=5$

$$1+2+3+4=10=2.5$$
$$1.2+1.3+1.4+2.3+2.4+3.4=35=7.5$$
$$1.2.3+1.2.4+1.3.4+2.3.4=50=10.5$$
$$1.2.3.4=14=3.5-1$$

VII. Aus der oben bei II. vorgenommenen Zerlegung der Kongruenz (1) vom Grade n, wobei sich so viel Faktoren vom ersten Grade in der Form $x-x_1$, $x-x_2\ldots$ absondern liessen, als die Kongruenz Wurzeln hat, geht hervor, dass wenn eine zweite ähnliche Kongruenz vom Grade m gewisse Wurzeln mit der ersteren gemein hat, sich von derselben die entsprechenden gleichen Faktoren werden absondern lassen.

Nimmt man also von den beiden Funktionen, welche die linken Seiten dieser beiden Kongruenzen bilden, nach bekannten Regeln der Algebra das grösste gemeinschaftliche Maass (wobei man dafür zu sorgen hat, dass die Koeffizienten der Quotienten in den zu diesem Zwecke anzustellenden Divisionen stets ganze Zahlen werden); so muss, wenn man dieses gemeinschaftliche Maass $\equiv 0$ setzt, die sich ergebende Kongruenz offenbar die den beiden gegebenen Kongruenzen ge-

meinschaftlich zukommenden Wurzeln enthalten. Es kann sich übrigens ereignen, dass der Grad des gemeinschaftlichen Maasses, also auch der Grad der resultirenden Kongruenz mehr Einheiten enthält, als gemeinschaftliche Wurzeln vorhanden sind, in welchem Falle die linke Seite der resultirenden Kongruenz aus einem Produkte von der Form $(x-x_1)(x-x_2)\ldots$ und einem beiden gegebenen Kongruenzen gemeinschaftlich angehörigen unlösbaren Polynome bestehen wird.

Der Satz VI. gibt aber ein Mittel, die Anzahl der verschiedenen Wurzeln der Kongruenz (1) vom $n$ten Grade genau zu bestimmen. Denn alle m Wurzeln, welche diese Kongruenz vom $n$ten Grade enthält, kommen offenbar auch der Kongruenz (14) vom $p-1$ten Grade zu. Ermittelt man also das grösste gemeinschaftliche Maass zwischen

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \text{ und } x^{p-1}-1$$

und setzt dasselbe $\equiv 0$; so muss die entstehende Kongruenz die m Wurzeln enthalten, welche den Kongruenzen (1) und (14) gemeinschaftlich angehören. Das fragliche gemeinschaftliche Maass ist aber ein Faktor von $x^{p-1}-1$, und enthält demnach genau so viel verschiedene Wurzeln, als sein Grad Einheiten. Demnach muss der Grad der resultirenden Kongruenz $=m$ sein, also genau die Anzahl der verschiedenen Wurzeln der Kongruenz (1) anzeigen.

Wäre zwischen den beiden genannten Polynomen kein gemeinschaftliches Maass vorhanden; so hätte die gegebene Kongruenz (1) auch keine Wurzeln.

§. 147. *Die quadratischen Reste und die Grundbedingung ihrer Existenz, wenn der Model eine Primzahl ist.*

I. Ein besonderes Interesse erwecken die reinen quadratischen Kongruenzen $x^2-a\equiv 0 \mod p$, welche man auch in der Form

$$(1) \qquad a \equiv x^2 \mod p$$

schreiben kann. Nach dieser Form wird also eine Zahl x gesucht, deren Quadrat zu der gegebenen Zahl a nach dem Model p kongruent ist. Statt dieser Kongruenz hat man auch die Gleichung

$$(2) \qquad a = x^2 + wp \quad \text{oder} \quad a - x^2 = wp$$

welcher zufolge ein Werth von x gesucht wird, der die Zahlform $a-x^2$ durch p theilbar macht.

Wegen der wichtigen Beziehungen, welche zwischen den beiden Zahlen a und p bestehen, sind dieselben von Gauss mit besonderen Namen belegt. Nach dessen Vorgange nennt man die Zahl a, welche fähig ist, nach dem Model p irgend

einem Quadrate kongruent oder der Rest irgend eines Quadrats zu werden, einen quadratischen Rest der Zahl p. Wenn dagegen die Zahl a hierzu unfähig, also die Kongruenz (1) unmöglich ist; so heisst a ein quadratischer Nichtrest von p. Dass a ein quadratischer Rest oder Nichtrest von p sei, bezeichnet Gauss kurz resp. durch die Formel

$$aRp \quad \text{oder} \quad aNp$$

Man findet, dass die vorstehende, mit Rücksicht auf Kürze des Ausdrucks von Gauss gewählte Benennung der Zahl a nicht ganz streng in dem Prinzipe der Nomenklatur des §. 135, I. für die Kongruenzen ersten Grades begründet ist, indem bei gewöhnlichen Resten oder denen vom ersten Grade die beiden kongruenten Zahlen miteinander, bei quadratischen Resten dagegen die Eine dieser Zahlen mit dem Model verglichen worden. Wenngleich durch die abweichende Benennung der quadratischen Reste nicht leicht Missverständnisse zu besorgen sind; so fragt es sich dennoch, ob es der Konsequenz wegen nicht rathsam sei, unter strenger Beibehaltung der Begriffe des §. 135, I. zu sagen, a sei ein quadratischer Rest nach p (statt von p). Wir werden uns in allem Folgenden stets dieser konsequenteren Benennung bedienen.

II. Wenn p eine in a nicht aufgehende unpaare positive Primzahl ist; so lautet die Grundbedingung für die Möglichkeit oder Unmöglichkeit der Kongruenz (1) folgendermaassen.

Die Zahl a ist ein quadratischer Rest oder Nichtrest nach p, je nachdem man hat

$$(3) \qquad a^{\frac{p-1}{2}} \equiv 1 \quad \text{oder} \quad \equiv -1 \mod p$$

und im ersteren Falle gibt es für x immer einen Werth, absolut kleiner als $\frac{p}{2}$, welcher die Kongruenz

$$(4) \qquad a \equiv x^2 \mod p$$

erfüllt.

Zum Beweise dieses äusserst wichtigen Satzes denken wir uns die Quadrate der natürlichen Zahlen von 1 bis $p-1$ gebildet und deren kleinste positive Reste nach dem Model p genommen, sodass man resp.

$$x^2 = 1^2, 2^2, 3^2 \ldots (p-1)^2 \equiv r_1, r_2, r_3 \ldots r_{p-1}$$

hat. Von diesen $p-1$ Resten werden je zwei von den Enden gleich weit abstehende wie r_n und r_{p-n} einander gleich sein,

weil man offenbar $(p-n)^2 = p^2 + 2pn + n^2 \equiv n^2$ hat. Lässt man aber die zweite Hälfte dieser Reste, welche der ersten Hälfte gleich sind, ausser Acht, betrachtet also nur die $\frac{p-1}{2}$ Reste der Quadrate von $1, 2, 3 \ldots \frac{p-1}{2}$; so werden dieselben sämmtlich verschieden sein. Denn wären zwei Reste dieser Hälfte, wie r_m und r_n einander gleich, wäre also $m^2 \equiv n^2$ oder $m^2 - n^2 = (m+n)(m-n) \equiv 0 \mod p$; so müsste entweder die Zahl $m+n$ oder die Zahl $m-n$ durch p theilbar sein, was unmöglich ist, da beide Zahlen $< p$ sind.

Erwägt man nun, dass die Reste $r_1, r_2 \ldots r_{\frac{p-1}{2}}$ sämmtlich den Zahlen $1, 2, 3 \ldots p-1$ angehören; so leuchtet ein, dass von den natürlichen Zahlen $1, 2 \ldots p-1$ die Hälfte irgend einem Quadrate kongruent, also quadratische Reste sind, während die andere Hälfte keinem Quadrate kongruent, also quadratische Nichtreste sind.

Denken wir uns jetzt die natürlichen Zahlen $1, 2, 3 \ldots p-1$ auf die Potenz vom Grade $\frac{p-1}{2}$ erhoben; so wird eine jede dieser $p-1$ Potenzen entweder $\equiv 1$ oder $\equiv -1 \mod p$ sein (§. 139, III.). Da es nun nach §. 146, V. höchstens $\frac{p-1}{2}$ Zahlen geben kann, deren $\frac{p-1}{2}$te Potenzen einander kongruent sind; so muss offenbar die Hälfte der erwähnten Potenzen $\equiv 1$ und die andere Hälfte $\equiv -1$ sein.

Es ist aber die $\frac{p-1}{2}$te Potenz eines jeden der vorhin mit r bezeichneten quadratischen Reste $\equiv 1$; denn man hat $r_n^{\frac{p-1}{2}} \equiv (n^2)^{\frac{p-1}{2}} = n^{p-1}$, welcher Werth nach dem Fermatschen Lehrsatze §. 139 stets $\equiv 1$ ist.

Da nun die Menge der verschiedenen Werthe der Reste r gleich $\frac{p-1}{2}$ ist; so erhellet, dass diese quadratischen Reste diejenige Hälfte der Zahlen $1, 2, 3 \ldots p-1$ darstellen, deren $\frac{p-1}{2}$te Potenzen $\equiv 1$ sind, während die Potenzen der anderen Hälfte oder der quadratischen Nichtreste $\equiv -1$ sind.

Hieraus folgt, dass eine Zahl a, deren $\frac{p-1}{2}$te Potenz $\equiv 1$ ist (und für welche man in der Formel (3) auch ihren

kleinsten positiven Rest nach p gesetzt denken kann) nothwendig irgend Einem der quadratischen Reste oder einem Quadrate x^2 kongruent sein, also selbst einen quadratischen Rest darstellen muss, während im anderen Falle eine Zahl a, deren $\frac{p-1}{2}$te Potenz $\equiv -1$ ist, nur ein quadratischer Nichtrest sein kann.

Unter den positiven Zahlen $1, 2 \ldots p-1$ gibt es nach Vorstehendem aber immer zwei, deren Quadrate $\equiv a$ sind. Ist x die Eine; so ist $p-x$ die andere. Beide sind $< p$; die Eine aber ist sogar $< \frac{p}{2}$, während die andere $> \frac{p}{2}$ ist. Die erste stellt den absolut kleinsten Werth von x dar, und man kann offenbar, wenn x die Eine ist, $-x$ für die andere nehmen.

Der umgekehrte Satz, dass die $\frac{p-1}{2}$te Potenz von a kongruent 1 oder -1 sei, jenachdem a ein quadratischer Rest oder Nichtrest nach p ist, leuchtet hiernach von selbst ein.

Die Primzahl p kann in Vorstehendem auch negativ gedacht werden, wenn man nur in dem Exponenten $\frac{p-1}{2}$ unter p den absoluten oder positiven Werth jener Primzahl versteht.

§. 148. *Das Reziprozitätsgesetz.*

I. Mit diesem Namen hat Legendre einen von ihm zuerst aufgefundenen, aber ohne genügenden Beweis aufgestellten Satz belegt, welcher sich folgendermaassen darstellen lässt: Wenn p und q zwei unpaare und verschiedene positive Primzahlen sind, und man setzt

$$(1) \qquad q^{\frac{p-1}{2}} \equiv (-1)^m \mod q$$

$$(2) \qquad p^{\frac{q-1}{2}} \equiv (-1)^n \mod q$$

so ist

$$(3) \qquad m+n = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Ist also Eine der Zahlen p, q oder sind beide von der Form $4r+1$, ist mithin $\frac{p-1}{2} \cdot \frac{q-1}{2}$ eine paare Zahl; so sind m und n entweder beide paar oder beide unpaar, folglich immer $(-1)^m = (-1)^n$.

Ist dagegen keine der Zahlen p, q von der Form $4r+1$,

sind vielmehr beide von der Form $4r+3$, ist mithin $\frac{p-1}{2}.\frac{q-1}{2}$ eine unpaare Zahl; so ist von m und n die Eine paar und die andere unpaar, folglich $(-1)^m = -(-1)^n$.

Hiernach lautet das Reziprozitätsgesetz: Wenn sich unter den beiden unpaaren Primzahlen p, q Eine von der Form $4r+1$ findet; so haben die absolut kleinsten Reste von $q^{\frac{p-1}{2}}$ und $p^{\frac{q-1}{2}}$ resp. für die Model p und q **gleiche** Zeichen; wenn dagegen jene Zahlen beide von der Form $4r+3$ sind; so haben jene Reste **ungleiche** Zeichen.

II. Zum Beweise dieses Satzes bilden wir zuerst für den Model p folgende Gruppe von Gleichungen und korrespondirenden Kongruenzen für die sukzessiven Vielfachen der Zahl q, indem wir die kleinsten positiven Reste mit R bezeichnen und zur Abkürzung

$$\frac{p-1}{2} = v \qquad \frac{q-1}{2} = w \qquad \text{also}$$
$$p-1 = 2v \qquad q-1 = 2w$$

setzen, und demnach die Beziehung $m+n = vw$ zu beweisen suchen.

$$\begin{array}{rclcrcl}
 & (A) & & & & (A) & \\
1q &=& V_1p + R_1 & & 1q &\equiv& R_1 \ mod\,p \\
2p &=& V_2p + R_2 & & 2q &\equiv& R_2 \\
3q &=& V_3p + R_3 & & 3q &\equiv& R_3 \\
 &\vdots& & & &\vdots& \\
vq &=& V_vp + R_v & & vq &\equiv& R_v \\
 &\vdots& & & &\vdots& \\
2vq &=& V_{2v}p + R_{2v} & & 2vq &\equiv& R_{2v}
\end{array}$$

Unter der obersten Hälfte dieser Reste, also unter den Resten $R_1, R_2 \ldots R_v$, welche sämmtlich $<p$ sind, kommt eine gewisse Anzahl m vor, welche $>\frac{p}{2}$ sind, während die übrigen $<\frac{p}{2}$ sind. Es werden dann unter der untersten Hälfte, also unter den Resten $R_{v+1}, R_{v+2}, \ldots R_{2v}$ eine Anzahl m vorkommen, welche $<\frac{p}{2}$ sind, während die übrigen $>\frac{p}{2}$ sind. Da nun immer je zwei Reste von den Zeigern x und $p-x$ die Summe p bilden (§. 136); so ist klar, dass die m Reste der oberen Hälfte, welche $>\frac{p}{2}$ sind, mit den m Resten der unteren Hälfte,

welche $<\frac{p}{2}$ sind, dergestalt korrespondiren, dass je Einer der ersteren mit je Einem der letzteren sich zu dem Werthe p ergänzt. Wären also R_a, R_b, $R_c \ldots$ die m Reste der unteren Hälfte, welche $<\frac{p}{2}$ sind; so würden die m Reste der oberen Hälfte, welche $>\frac{p}{2}$ sind, $p-R_a$, $p-R_b$, $p-R_c \ldots$ sein.

Ferner leuchtet ein, dass wenn man alle $v-m$ Reste aus der oberen Hälfte, welche $<\frac{p}{2}$ sind, und die m Reste R_a, R_b, $R_c \ldots$ aus der unteren Hälfte, welche ebenfalls $<\frac{p}{2}$ sind, zusammenschreibt, v Zahlen erhalten werden, welche sämmtlich $<\frac{p}{2}$ und voneinander verschieden sind, welche also, abgesehen von der Reihenfolge, alle Zahlen $1, 2, 3 \ldots v$ enthalten.

Setzt man nun an die Stelle der m Reste in der oberen Hälfte, welche $>\frac{p}{2}$ sind, die Werthe $p-R_a$, $p-R_b$, $p-R_c \ldots$; so erhält man für irgend Eine der betreffenden Gleichungen (A) einen Ausdruck von der Form

(4) $tq \equiv Vp + R = Vp + p - R_a = (V+1)p - R_a$ also

(5) $tq \equiv -R_a$

Multiplizirt man, nachdem man die hierdurch sich ergebenden m neuen Kongruenzen, deren rechte Seiten negativ sind, für die betreffenden m der früheren Kongruenzen substituirt hat, alle v Kongruenzen der oberen Hälfte der Gruppe (A) mit einander; so ergibt sich

$$1.2.3 \ldots v q^v \equiv (-1)^m 1.2.3 \ldots v \bmod p$$

also, da $1.2.3 \ldots v$ eine zum Model p relativ prime Zahl ist, durch welche die vorstehende Kongruenz dividirt werden kann,

(6) $q^v \equiv (-1)^m \bmod p$

Addirt man dagegen die korrespondirenden v Gleichungen der oberen Hälfte, indem man für die fraglichen m Gleichungen von der Form (4) die gleichbedeutenden in der Form

(7) $tq = Vp + p + R_a - 2R_a$

substituirt; so ergibt sich, da die Summe der Zahlen

$$1 + 2 + 3 + \ldots + v = \frac{v(v+1)}{2}$$

ist,

$$\frac{v(v+1)}{2}q = (V_1+V_2+\ldots+V_v)p + mp + \frac{v(v+1)}{2}$$
$$-2(R_a+R_b+R_c+\ldots)$$

oder durch Transposition

(8) $(V_1+V_2+\ldots+V_v+m)p = v(v+1)w + 2(R_a+R_b+R_c+\ldots)$

Da von den beiden Zahlen v und $v+1$ stets Eine paar ist; so folgt, dass die ganze rechte Seite der vorstehenden Gleichung paar ist; Demnach muss auch die linke Seite paar sein, und da p unpaar ist, muss $V_1+V_2+\ldots+V_v+m$ paar sein. Hieraus geht hervor, dass die beiden Zahlen

$$m \text{ und } V_1+V_2+\ldots+V_v$$

zu gleicher Zeit entweder paar oder unpaar sind.

III. Bilden wir jetzt für q als Model in ähnlicher Weise die Gleichungen und Kongruenzen

$$\begin{array}{rclcrcl} & (B) & & \qquad & & (B) & \\ 1p &=& W_1q+S_1 & & 1p &\equiv& S_1 \mod q \\ 2p &=& W_2q+S_2 & & 2p &\equiv& S_2 \\ 3p &=& W_3q+S_3 & & 3p &\equiv& S_3 \\ &\vdots& & & &\vdots& \\ wp &=& W_wq+S_w & & wp &\equiv& S_w \\ &\vdots& & & &\vdots& \\ 2wp &=& W_{2w}q+S_{2w} & & 2wp &\equiv& S_{2w} \end{array}$$

und ertheilen in Beziehung auf diese Gruppe (B) der Zahl n eine Bedeutung, welche der der Zahl m in Beziehung auf die Gruppe (A) entspricht; so folgt, dass

(9) $$p^w \equiv (-1)^n \mod q$$

ist, und dass auch die beiden Zahlen

$$n \text{ und } W_1+W_2+\ldots+W_w$$

zu gleicher Zeit paar oder unpaar sind.

IV. Hieraus und aus dem Obigen ist klar, dass die beiden Zahlen

$$m+n \text{ und } (V_1+V_2+\ldots+V_v)+(W_1+W_2+\ldots+W_w)$$

zu gleicher Zeit paar oder unpaar sind. Man kann also in Absicht auf den zu erweisenden Lehrsatz (3), bei welchem es nur darauf ankommt, ob m und n paar oder unpaar ist, den Werth

$$\begin{array}{ll} V_1+V_2+\ldots+V_v & \text{für } m \text{ und} \\ W_1+W_2+\ldots+W_w & \text{für } n \end{array}$$

nehmen.

V. Um jetzt den Werth der für $m+n$ zu nehmenden Summe der Grössen V und W zu bestimmen; so sei $q<p$. Dividirt man jede in der oberen Hälfte der Gruppe (A) stehende Gleichung durch p; so kommt

(C)

$$1\frac{q}{p}=V_1+\frac{R_1}{p}$$

$$2\frac{q}{p}=V_2+\frac{R_2}{p}$$

$$3\frac{q}{p}=V_3+\frac{R_3}{p}$$

$$\vdots$$

$$v\frac{q}{p}=V_v+\frac{R_v}{p}$$

Hierin sind alle Brüche $\frac{R_1}{p}$, $\frac{R_2}{p}$, $\frac{R_3}{p}\ldots$ auf der rechten Seite echt, also V_1, V_2, $V_3\ldots$ die grössten resp. in den Brüchen $\frac{q}{p}$, $\frac{2q}{p}$, $\frac{3q}{p}\ldots$ enthaltenen Ganzen.

VI. Dividirt man nun auch jede in der oberen Hälfte der Gruppe (B) stehende Gleichung durch p; so kommt

(D)

$$1=W_1\frac{q}{p}+\frac{S_1}{p}$$

$$2=W_2\frac{q}{p}+\frac{S_2}{p}$$

$$3=W_3\frac{q}{p}+\frac{S_3}{p}$$

$$\vdots$$

$$w=W_w\frac{q}{p}+\frac{S_w}{p}$$

Da alle mit S bezeichneten Reste $<q$ sind und $q<p$ ist; so sind auch alle jene Reste $<p$, folglich $\frac{S_1}{p}$, $\frac{S_2}{p}$, $\frac{S_3}{p}\ldots$ lauter echte Brüche. Transponirt man dieselben auf die andere Seite; so ergeben sich folgende Gleichungen.

$$W_1\frac{q}{p}=1-\frac{S_1}{p}$$

$$W_2\frac{q}{p}=2-\frac{S_2}{p}$$

$$W_3\frac{q}{p}=3-\frac{S_3}{p}$$

$$\vdots$$

$$W_w\frac{q}{p}=w-\frac{S_w}{p}$$

Aus diesen Gleichungen ergeben sich sofort die nachstehenden.

$$W_1\frac{q}{p}=0+\left(1-\frac{S_1}{p}\right) \quad \text{und} \quad (W_1+1)\frac{q}{p}=1+\left(\frac{q}{p}-\frac{S_1}{p}\right)$$

$$W_2\frac{q}{p}=1+\left(1-\frac{S_2}{p}\right) \qquad (W_2+1)\frac{q}{p}=2+\left(\frac{q}{p}-\frac{S_2}{p}\right)$$

$$W_3\frac{q}{p}=2+\left(1-\frac{S_3}{p}\right) \qquad (W_3+1)\frac{q}{p}=3+\left(\frac{q}{p}-\frac{S_3}{p}\right)$$

$$\vdots \qquad\qquad \vdots$$

$$W_w\frac{q}{p}=w-1+\left(1-\frac{S_w}{p}\right) \qquad (W_w+1)\frac{q}{p}=w+\left(\frac{q}{p}-\frac{S_w}{p}\right)$$

Hierin sind sowol $\left(1-\frac{S_1}{p}\right)$, $\left(1-\frac{S_2}{p}\right)$, ... wie auch $\left(\frac{q}{p}-\frac{S_1}{p}\right)$, $\left(\frac{q}{p}-\frac{S_2}{p}\right)$... lauter **positive echte** Brüche, und es ist klar, dass folgende Gleichungen bestehen.

(E)

$$1\frac{q}{p}=0+ \text{ einem echten Bruche}$$

$$2\frac{q}{p}=0+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$\vdots$$

$$W_1\frac{q}{p}=0+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$(W_1+1)\frac{q}{p}=1+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$(W_1+2)\frac{q}{p}=1+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$\vdots$$

$$W_2\frac{q}{p}=1+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$(W_2+1)\frac{q}{p}=2+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$(W_2+2)\frac{q}{p}=2+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$\vdots$$

$$W_3\frac{q}{p}=2+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$(W_3+1)\frac{q}{p}=3+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$(W_3+2)\frac{q}{p}=3+ \quad \text{»} \quad \text{»} \quad \text{»}$$

$$\vdots$$

$$W_4\frac{q}{p} = 3 + \text{einem echten Bruche}$$

. . . .
. . . .
. . . .

$$(W_w + 1)\frac{q}{p} = w + \quad » \quad » \quad »$$
$$(W_w + 2)\frac{q}{p} = w + \quad » \quad » \quad »$$
$$\vdots$$
$$W_{w+1}\frac{q}{p} = w + \quad » \quad » \quad »$$

VII. Auf der linken Seite dieser Gleichungen kommen die Zahlwerthe $1\frac{q}{p}$, $2\frac{q}{p}$, $3\frac{q}{p} \ldots v\frac{q}{p}$ in der natürlichen Reihenfolge der davor stehenden Koeffizienten vor, und zwar liegt der letzte Werth $v\frac{q}{p}$ in der letzten Abtheilung der Gruppe (E), welche sich von dem Werthe

$$(W_w + 1)\frac{q}{p} \quad \text{bis} \quad W_{w+1}\frac{q}{p}$$

erstreckt. Um diese Behauptung einzusehen, beachte man, dass der Koeffizient des Werthes, welcher der eben genannten Abtheilung unmittelbar vorhergeht, kleiner als v, dass also

$$W_w < v$$

ist. Dies folgt sofort aus der Gleichung $wp = W_w q + S_w$ der Gruppe (B). Nach dieser Gleichung hat man nämlich

$$W_w = v - \frac{2S_w + (p - q)}{2q}$$

worin die von v zu subtrahirende Grösse positiv ist, weil man $p > q$ hat.

Der Koeffizient der letzten Gleichung der Gruppe (E) ist aber grösser als v, also

$$W_{w+1} > v$$

Denn aus der Gleichung $(w + 1)p = W_{w+1}q + S_{w+1}$ der Gruppe (B) folgt

$$W_{w+1} = v + \frac{(p - S_{w+1}) + (q - S_{w+1})}{2q}$$

worin die zu v zu addirende Grösse positiv ist, weil sowol p, wie auch q grösser als S_{w+1} ist.

VIII. Bricht man also die Gruppe (E) mit der in ihrer letzten Abtheilung liegenden Gleichung

$$v\frac{q}{p} = w + \text{einem echten Bruche}$$

ab; so muss dieselbe ganz identisch mit der Gruppe (C) sein. Demnach hat man durch Vergleichung der grössten Ganzen auf den rechten Seiten der beiden Gruppen (C) und (E) resp.

$V_1,\ V_2,\ V_3,\ V_4 \ldots V_v = 0,\ 0 \ldots 0,\ 1,\ 1 \ldots 1,\ 2,\ 2 \ldots 2 \ldots w,\ w \ldots w$

Nach Maassgabe der Gruppe (E) erscheint unter diesen Werthen von $V_1,\ V_2 \ldots V_v$

die	Zahl	0	überhaupt	W_1	mal
»	»	1	»	$W_2 - W_1$	»
»	»	2	»	$W_3 - W_2$	»
»	»	3	»	$W_4 - W_3$	»
		⋮			
»	»	w	»	$v - W_w$	»

Addirt man also alle jene Grössen V; so kommt

$$V_1 + V_2 + V_3 + \ldots + V_v$$
$$= 0 . W_1 + 1(W_2 - W_1) + 2(W_3 - W_2) + \ldots + (w-1)(W_w - W_{w-1}) + w(v - W_w)$$
$$= \quad 0 . W_1 + 1 W_2 + 2 W_3 + \ldots + (w-1) W_w + vw$$
$$- 1 . W_1 - 2 W_2 - 3 W_3 - \ldots - w W_w$$
$$= -(W_1 + W_2 + W_3 + \ldots + W_w) + vw$$

Hieraus folgt durch Transposition

(10) $(V_1 + V_2 + \ldots + V_v) + (W_1 + W_2 + \ldots + W_w) = vw$

und da für den Zweck des obigen Lehrsatzes statt der beiden Glieder auf der linken Seite resp. die beiden Zahlen m und n genommen werden können, indem es für die Letzteren nur darauf ankommt, ob sie paar oder unpaar sind, so ergibt sich die zu erweisende Beziehung

(11) $$m + n = vw = \frac{p-1}{2} . \frac{q-1}{2}$$

Zu vorstehender Entwickelung hat der in Legendres *Théorie des nombres, sec. éd. §. VII.* mitgetheilte Beweis von Gauss den Antrieb gegeben. Das gegenwärtige Verfahren dürfte wegen der darin liegenden Kürze und Allgemeinheit, da es von der speziellen Form der Zahlen p, q völlig unabhängig ist, einige Beachtung verdienen.

IX. Legendre bezeichnet den kleinsten Rest von $q^{\frac{p-1}{2}}$

nach dem Model p kurz mit $\left(\frac{q}{p}\right)$, sodass man also nach dieser Bezeichnung

(12) $$\left(\frac{q}{p}\right)=\pm 1$$

hat. Hiernach ist das Reziprozitätsgesetz in der Formel

(13) $$\left(\frac{q}{p}\right)=\pm\left(\frac{p}{q}\right)$$

enthalten, worin das obere oder untere Zeichen gilt, jenachdem irgend Eine oder keine der beiden ungeraden positiven Primzahlen p, q von der Form $4r+1$ ist.

So ist z. B. $\left(\frac{17}{29}\right)=\left(\frac{29}{17}\right)$, auch $\left(\frac{5}{31}\right)=\left(\frac{31}{5}\right)$, dagegen $\left(\frac{11}{23}\right)=-\left(\frac{23}{11}\right)$.

X. Es ist bisher vorausgesetzt, dass p und q positiv seien. Was den Fall betrifft, wo Eine dieser Zahlen oder beide negativ, jedoch immer unpaar, seien; so ist zuvörderst klar, dass der im Nenner des Ausdrucks $\left(\frac{q}{p}\right)$ stehende Model p ohne Einfluss auf den Werth dieses Ausdrucks sowol positiv, wie negativ sein kann, dass man also stets $\left(\frac{q}{-p}\right)=\left(\frac{q}{p}\right)$ hat.

Wenn jedoch die im Zähler stehende Primzahl q ihr Zeichen wechselt; so ändert der ganze Ausdruck sein Zeichen nicht, wenn der absolute Werth des Models p von der Form $4r+1$ ist, wohl aber dann, wenn der absolute Werth von p die Form $4r+3$ hat. Im ersteren Falle ist also $\left(\frac{-q}{p}\right)=\left(\frac{q}{p}\right)$; im letzteren dagegen $\left(\frac{-q}{p}\right)=-\left(\frac{q}{p}\right)$.

So hat man z. B. nach diesem Satze und dem Reziprozitätsgesetze

$$\left(\frac{-17}{29}\right)=\left(\frac{17}{29}\right)=\left(\frac{29}{17}\right)$$
$$\left(\frac{-5}{31}\right)=-\left(\frac{5}{31}\right)=-\left(\frac{31}{5}\right)$$
$$\left(\frac{-11}{23}\right)=-\left(\frac{11}{23}\right)=\left(\frac{23}{11}\right)$$

XI. Wenn q eine ganz beliebige Zahl und p eine in q nicht aufgehende ungerade Primzahl ist; so behält die obige

Deduktion von der Gruppe (A) bis zu der Gleichung (6) vollkommene Gültigkeit. Dies ist von Wichtigkeit: denn wenn es bloss darauf ankommt, zu entscheiden, ob $q^{\frac{p-1}{2}} \equiv +1$ oder $\equiv -1 \; mod \, p$ sei; so hat man nicht nöthig, die Reste der aufsteigenden Potenzen von q bis zu der $\frac{p-1}{2}$ten zu bilden. Man braucht vielmehr nach Gl. (6) nur nachzusehen, wie viel Reste R der sukzessiven Vielfachen von q in der oberen Hälfte der Gruppe (A), also wie viel der Reste $R_1, R_2 \ldots R_{\frac{p-1}{2}}$ grösser als $\frac{p}{2}$ sind. Ist deren Anzahl $= m$; so hat man ohne Weiteres $q^{\frac{p-1}{2}} \equiv (-1)^m \; mod \, p$.

XII. Es ist noch zu bemerken, dass eine Addition der Gleichungen der Gruppe (A) und der Gruppe (B) folgende Beziehung für die Summe der Quotienten V oder W ergibt.

$$(14) \quad V_1 + V_2 + \ldots + V_{p-1} = W_1 + W_2 + \ldots + W_{q-1} = \frac{(p-1)(q-1)}{2}$$

XIII. Bei den obigen Untersuchungen ist der Fall ausgeschlossen gewesen, wo irgend Eine der beiden Primzahlen p, q den absoluten Werth 2 hat. Dieser Fall führt zu folgenden Gesetzen.

Ist in dem Ausdrucke $\left(\frac{q}{p}\right)$ der absolute Werth des Models $p = 2$; so ist für jede unpaare Primzahl q jede Potenz von q sowol $\equiv 1$, als auch $\equiv -1 \; mod \; 2$.

Ist dagegen $q = 2$; so hat man, wenn der absolute Werth des Models p von der Form $8r+1$ oder $8r+7$ (d. i. von Einer der Formen $8r \pm 1$) ist,

$$(15) \qquad 2^{\frac{p-1}{2}} \equiv 1 \; mod \, p \quad \text{oder} \quad \left(\frac{2}{p}\right) = 1$$

wenn dagegen der absolute Werth des Models p von der Form $8r+3$ oder $8r+5$ (d. i. von Einer der Formen $8r \pm 3$) ist,

$$(16) \qquad 2^{\frac{p-1}{2}} \equiv -1 \; mod \, p \quad \text{oder} \quad \left(\frac{2}{p}\right) = -1$$

Denn allgemein wird für diesen Fall die obere Hälfte der Kongruenzen der Gruppe (B)

$$\begin{aligned} 1 \,.\, 2 &\equiv 2 \mod p \\ 2 \,.\, 2 &\equiv 4 \\ 3 \,.\, 2 &\equiv 6 \\ &\vdots \\ \frac{p-1}{2} \,.\, 2 &\equiv p-1 \end{aligned}$$

Wenn nun $p = 8r + 1$ oder $= 8r + 5$, also $\frac{p-1}{2}$ eine paare Zahl ist; so sind von diesen Resten die obere Hälfte $< \frac{p}{2}$ und die untere Hälfte $> \frac{p}{2}$. Die Anzahl der Reste in einer jeden dieser beiden Hälften ist aber $= \frac{p-1}{4}$, also paar, wenn $p = 8r + 1$ ist, und unpaar, wenn $p = 8r + 5$ ist.

Wenn dagegen $p = 8r + 3$ oder $= 8r + 7$, also $\frac{p-1}{2}$ eine unpaare Zahl ist; so sind die oberen $\left(\frac{p-1}{4} - \frac{1}{2}\right)$ Reste $< \frac{p}{2}$ und die unteren $\left(\frac{p-1}{4} + \frac{1}{2}\right)$ oder $\frac{p+1}{4}$ Reste $> \frac{p}{2}$. Die Anzahl der letzteren ist aber unpaar, wenn $p = 8r + 3$ ist, und paar, wenn $p = 8r + 7$ ist.

Sobald nun die Anzahl der Reste, welche $> \frac{p}{2}$ sind, paar ist, gilt nach (9) die Kongruenz (15); sobald aber jene Anzahl unpaar ist, die Kongruenz (16).

Die beiden Kongruenzen (15) und (16) lassen sich in eine einzige Formel bringen, wenn man den absoluten Werth der Primzahl p in der Form $4s \pm 1$ darstellt, in welcher derselbe offenbar stets enthalten ist. Man hat dann allgemein

(17) $$2^{\frac{p-1}{2}} \equiv (-1)^s \mod p$$

XIV. Ist ferner $q = -2$; so führen die soeben gefundenen Beziehungen, in Verbindung mit der Regel X. leicht zu folgenden Sätzen.

Wenn der absolute Werth des Models p von der Form $8r + 1$ oder $8r + 3$ ist; so hat man

(18) $$(-2)^{\frac{p-1}{2}} \equiv 1 \mod p \quad \text{oder} \quad \left(\frac{-2}{p}\right) = 1$$

und wenn der absolute Werth des Models p von der Form $8r + 5$ oder $8r + 7$ ist; so hat man

(19) $(-2)^{\frac{p-1}{2}} \equiv -1 \bmod p$ oder $\left(\frac{-2}{p}\right) = -1$

XV. Auch der Fall, wo p oder q den absoluten Werth 1 hat, verdient noch hervorgehoben zu werden.

Ist der absolute Werth des Models $p = 1$; so ist jede Potenz von $q \equiv 0 \bmod 1$.

Ist ferner $q = 1$; so ist jede Potenz davon für jeden beliebigen Model $\equiv 1$ und für den speziellen Model 2 auch noch $\equiv -1$.

Ist aber $q = -1$; so ist für jede Primzahl p, deren absoluter Werth die Form $4r+1$ hat,

(20) $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$ oder $\left(\frac{-1}{p}\right) = 1$

und für jede Primzahl p, deren absoluter Werth die Form $4r+3$ hat,

(21) $(-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$ oder $\left(\frac{-1}{p}\right) = -1$

§. 149. *Gauss's Fundamentalsatz für die Theorie der quadratischen Reste.*

I. In dem Reziprozitätsgesetze (§. 147) liegt folgende für die Lehre von den quadratischen Resten höchst wichtige Beziehung, welche Gauss zuerst aufgefunden und in den *Disquisitiones arithmeticae, art. 131* den Fundamentalsatz für die Theorie der quadratischen Reste genannt hat. Derselbe lautet unter der Voraussetzung, dass p und q zwei unpaare und positive Primzahlen seien:

Wenn p eine Primzahl von der Form $4r+1$ ist; so ist p quadratischer Rest oder Nichtrest nach jeder Primzahl q, welche resp. quadratischer Rest oder Nichtrest nach p ist.

Wenn dagegen p eine Primzahl von der Form $4r+3$ ist; so ist $-p$ quadratischer Rest oder Nichtrest nach jeder Primzahl q, welche resp. quadratischer Rest oder Nichtrest nach p ist.

In Zeichen ist also unter der Voraussetzung, dass $4r+1$, $4r+3$ und q ungerade positive Primzahlen seien,

(1) $\begin{cases} (4r+1)Rq, & \text{wenn } qR(4r+1) \text{ ist,} \\ (4r+1)Nq, & \text{»} \quad qN(4r+1) \quad \text{»} \end{cases}$

(2) $\begin{cases} -(4r+3)Rq, & \text{»} \quad qR(4r+3) \quad \text{»} \\ -(4r+3)Nq, & \text{»} \quad qN(4r+3) \quad \text{»} \end{cases}$

II. Beweis. Wenn $p=4r+1$; so ist nach dem Reziprozitätsgesetze (§. 148)

$$q^{\frac{p-1}{2}} \equiv (-1)^m \bmod p$$
$$p^{\frac{q-1}{2}} \equiv (-1)^m \bmod q$$

Ist nun $(-1)^m \equiv +1$; so ist nach §. 147, V. gleichzeitig

$$qRp \text{ und } pRq$$

Ist dagegen $(-1)^m = -1$; so ist nach jenem Paragraphen gleichzeitig

$$qNp \text{ und } pNq$$

Hierdurch sind die beiden Beziehungen (1) erwiesen.

Wenn $p=4r+3$ und zuvörderst $q=4s+1$, also $\frac{q-1}{2}=2s$ eine paare Zahl ist; so hat man nach dem Reziprozitätsgesetze

$$q^{\frac{p-1}{2}} \equiv (-1)^m \bmod p$$
$$p^{\frac{q-1}{2}} \equiv (-1)^m \bmod q, \text{ also auch } (-p)^{\frac{q-1}{2}} \equiv (-1)^m \bmod q$$

Hieraus folgt wie vorhin, wenn $(-1)^m = +1$ ist, dass gleichzeitig

$$qRp \text{ und } -pRq$$

und wenn $(-1)^m = -1$ ist, dass gleichzeitig

$$qNp \text{ und } -pNq$$

ist.

Wenn dagegen $p=4r+3$ und auch $q=4s+3$, also $\frac{q-1}{2}=2s+1$ eine unpaare Zahl ist; so hat man nach dem Reziprozitätsgesetze

$$q^{\frac{p-1}{2}} \equiv (-1)^m \bmod p$$
$$p^{\frac{q-1}{2}} \equiv (-1)^{m+1} \bmod q, \quad \text{also} \quad (-p)^{\frac{q-1}{2}} \equiv (-1)^m \bmod q$$

Ist nun $(-1)^m = +1$; so ist nach §. 147, V. gleichzeitig

$$qRp \text{ und } -pRq$$

Ist dagegen $(-1)^m = -1$; so ist gleichzeitig

$$qNp \text{ und } -pNq$$

Hierdurch sind die beiden Beziehungen (2) bewiesen.

III. Der erste Theil des obigen Fundamentalsatzes, wofür p von der Form $4r+1$ vorausgesetzt wird, hat auch folgenden Sinn: Wenn es Zahlen von der Form $q-x^2$ gibt, welche durch p theilbar sind; so gibt es auch Zahlen von der Form $p-x^2$, welche durch q theilbar sind: sonst aber nicht.

So gibt es z. B., da Zahlen von der Form $19-x^2$ vorhanden sind, welche sich durch $p=5$ theilen lassen, auch Zahlen von der Form $5-x^2$, welche durch 19 theilbar sind. Ebenso gibt es, da keine Zahlen von der Form $19-x^2$ existiren, welche sich durch $p=13$ theilen lassen, auch keine Zahlen von der Form $13-x^2$, welche durch 19 theilbar sind.

Der zweite Theil des Fundamentalsatzes, wofür p von der Form $4r+3$ vorausgesetzt wird, hat den Sinn: Wenn es Zahlen von der Form $q-x^2$ gibt, welche durch p theilbar sind; so gibt es auch Zahlen von der Form $-p-x^2$ oder von der Form $p+x^2$, welche durch q theilbar sind: sonst aber nicht.

Da es also z. B. Zahlen von der Form $19-x^2$ gibt, welche durch $p=3$ theilbar sind; so gibt es auch solche von der Form $3+x^2$, welche durch 19 theilbar sind. Da es aber keine Zahlen von der Form $19-x^2$ gibt, welche durch $p=7$ theilbar sind; so gibt es auch keine von der Form $7+x^2$, welche durch 19 theilbar sind.

IV. Bisher sind die beiden unpaaren Primzahlen p, q als positiv vorausgesetzt. Wäre Eine oder wären beide negativ; so geschieht die Zurückführung des Falles auf das obige Gesetz sehr leicht durch folgende Betrachtung.

Offenbar kann in dem Ausdrucke qRp oder qNp der rechts stehende Model p sowol positiv wie negativ genommen werden. Wenn also qRp; so ist auch $qR-p$, oder wenn qNp; so ist auch $qN-p$.

Wechselt aber die links stehende Grösse q ihr Zeichen; so hat Dies auf jenen Ausdruck dann keinen Einfluss, wenn der absolute Werth des Models p von der Form $4r+1$ ist. Für diesen Fall würde also, wenn qRp wäre, auch $-qRp$ sein, oder wenn qNp wäre, auch $-qNp$ sein. Ist dagegen der absolute Werth des Models p von der Form $4r+3$; so geht mit dem Zeichenwechsel von q das Symbol R in N oder das Symbol N in R über. Wäre also für diesen Fall qRp; so hätte man $-qNp$, oder wäre qNp; so hätte man $-qRp$.

Der Beweis dieser Beziehungen erhellet sofort aus den ähnlichen Gesetzen des §. 148, X.

V. Hiernach lassen sich alle Fälle des obigen Fundamentalsatzes in folgendes Schema bringen, wonach das Stattfinden irgend Einer der in eine Horizontalreihe neben einander gestellten vier Beziehungen immer die anderen drei nothwendig nach sich zieht.

q	p				
$4s+1$	$4r+1$	qRp	pRq	$-qRp$	$-pRq$
$4s+3$	$4r+1$	qRp	pRq	$-qRp$	$-pNq$
$4s+1$	$4r+3$	qRp	$-pRq$	$-qNp$	pRq
$4s+3$	$4r+3$	qRp	$-pRq$	$-qNp$	pNq

In jeder Horizontalreihe kann auch gleichzeitig das Symbol R in N und das Symbol N in R verwandelt, auch kann in jeder einzelnen Formel das Zeichen des Models nach Belieben umgekehrt werden.

VI. Für den Fall, dass Eine der beiden Primzahlen p, q den absoluten Werth 2 hätte, sind folgende Gesetze zu merken.

Hat der Model p den absoluten Werth 2; so ist klar, dass jede andere Primzahl q quadratischer Rest nach p ist, dass man also hat

(3) $$qR2$$

Ist dagegen $q=2$; so erhellet aus §. 148, XIII., dass q quadratischer Rest nach jeder Primzahl von der Form $8r+1$ oder $8r+7$, dagegen quadratischer Nichtrest nach jeder Primzahl von der Form $8r+3$ oder $8r+5$ ist, dass man also hat

(4) $$2R(8r+1) \quad \text{und} \quad 2R(8r+7)$$

(5) $$2N(8r+3) \quad » \quad 2N(8r+5)$$

VII. Ist ferner $q=-2$; so ergibt sich aus §. 148, XIV., dass q quadratischer Rest nach jeder Primzahl von der Form $8r+1$ oder $8r+3$, dagegen quadratischer Nichtrest nach jeder Primzahl von der Form $8r+5$ oder $8r+7$ ist, dass man also hat

(6) $$-2R(8r+1) \quad \text{und} \quad -2R(8r+3)$$

(7) $$-2N(8r+5) \quad » \quad -2N(8r+7)$$

VIII. Die Zahl 1 anlangend; so ist, wenn der Model p den absoluten Werth 1 hat, jede Zahl q quadratischer Rest nach p oder

(8) $$qR1$$

Ist ferner $q=1$; so ist q quadratischer Rest nach jeder Zahl p, also

(9) $$1Rp$$

Ist dagegen $q=-1$; so ist nach §. 148, XV. q quadratischer Rest nach jeder Primzahl p, deren absoluter Werth die Form $4r+1$ hat, aber quadratischer Nichtrest nach jeder Primzahl, deren absoluter Werth die Form $4r+3$ hat, also ist

(10) $$-1R(4r+1)$$

(11) $$-1N(4r+3)$$

§. 150. **Die quadratischen Reste nach zusammengesetzten Modeln.**

A. Wenn q unpaar und relativ prim zu D ist.

I. Für die im fünften Abschnitte vorgetragene Theorie der unbestimmten Gleichungen vom zweiten Grade ist es wichtig, mit Leichtigkeit darüber entscheiden zu können, ob es Zahlen von der Form $D - x^2$ gibt, welche durch eine gegebene Zahl q theilbar sind oder nicht, ob also die Kongruenz

(1) $$D \equiv x^2 \mod q$$

möglich sei oder nicht, d. h. ob D ein quadratischer Rest oder Nichtrest nach q sei.

Wir schicken die Bemerkung voraus, dass unter D sowol eine positive, wie auch eine negative Grösse verstanden werden kann. Der Model q braucht jedoch offenbar nur positiv gedacht zu werden. Will man indessen auch für q negative Werthe zulassen; so müssen für diese Grösse und ihre Faktoren da, wo sie in den nachstehenden Formeln in den Exponenten einer Potenz treten, ihre absoluten Werthe gesetzt werden.

Wenn q eine in D nicht aufgehende unpaare Primzahl ist; so ist nach §. 147 D nur dann quadratischer Rest nach q, wenn man hat

(2) $$D^{\frac{q-1}{2}} \equiv 1 \mod q$$

Wäre z. B. $D = 12$ und $q = 13$ gegeben; so müsste man, damit 12 ein quadratischer Rest nach 13 oder $12 - x^2$ durch 13 theilbar sei, $12^6 \equiv 1 \mod 13$ haben. Untersucht man den Bestand der letzteren Kongruenz nach §. 148, XI.; so hat man für die Reste der Vielfachen von 12 bis zum $\frac{13-1}{2} = 6$fachen hinauf

$$\begin{aligned} 1 \,.\, 12 &\equiv 12 \mod 13 \\ 2 \,.\, 12 &\equiv 11 \\ 3 \,.\, 12 &\equiv 10 \\ 4 \,.\, 12 &\equiv 9 \\ 5 \,.\, 12 &\equiv 8 \\ 6 \,.\, 12 &\equiv 7 \end{aligned}$$

Da hierunter $m = 6$ Reste $> \frac{13}{2}$ vorkommen; so ist $12^6 \equiv (-1)^6 \equiv 1$, also 12 ein quadratischer Rest nach 13.

Ein zweites, oftmals noch einfacheres Verfahren zur Entscheidung der eben erörterten Frage, ob D ein quadratischer Rest nach q sei oder nicht, wird in §. 151 vorgetragen werden.

Gehen wir jetzt zu den allgemeineren Fällen über, wo q eine zusammengesetzte, jedoch unpaare und zu D relativ prime Zahl ist.

II. Wenn q eine Potenz einer in D nicht aufgehenden unpaaren Primzahl r, also $q = r^n$ ist; so ist D dann,

aber auch nur dann ein quadratischer Rest nach q, wenn es ein solcher nach dem Primfaktor r ist, wenn man also hat

(3) $$D^{\frac{r-1}{2}} \equiv 1 \mod r$$

Um Dies zu beweisen, wollen wir den Satz darthun, dass wenn D ein quadratischer Rest nach irgend einer Potenz r^n von r ist, es auch ein solcher nach der nächst höheren, also nach r^{n+1} sein wird. Denn hat man

$$D \equiv x^2 \mod r^n, \quad \text{also} \quad D - x^2 = vr^n$$

so ist auch für irgend einen Werth von w

$$D - (x + wr^n)^2 = D - x^2 - 2wxr^n - w^2r^{2n} = (v - 2wx - w^2r^n)r^n$$

Da nun r eine nicht in D, wol aber in $D - x^2$, mithin nicht in x^2 und demnach auch nicht in x aufgehende unpaare Primzahl ist; so wird dieselbe auch nicht in $2x$ enthalten sein. Man kann also die ganze Zahl w stets so wählen, dass

$$v - 2wx = ur \quad \text{oder} \quad r \,.\, u + 2x \,.\, w = v$$

wird, worin u irgend eine ganze Zahl bezeichnet. Denn Dies ist eine unbestimmte Gleichung vom ersten Grade mit den beiden Unbekannten u und w, deren Koeffizienten r und $2x$ relativ prim sind.

Wenn aber w in vorstehender Weise bestimmt gedacht wird; so hat man

$$D - (x + wr^n)^2 = (ur - w^2r^n)r^n = (u - w^2r^{n-1})r^{n+1}$$

also

$$D \equiv (x + wr^n)^2 \mod r^{n+1}$$

Hieraus folgt, dass wenn D ein quadratischer Rest nach r ist, es auch ein solcher nach jeder höheren Potenz $r^2, r^3, r^4 \ldots$ von r sein wird.

Dass umgekehrt, wenn D kein quadratischer Rest nach r ist, es auch kein solcher nach r^n sein kann, leuchtet von selbst ein: denn gibt es keine durch r theilbare Zahl von der Form $D - x^2$; so kann es auch keine durch r^n theilbare Zahl von dieser Form geben.

III. Wenn q das Produkt mehrerer in D nicht aufgehender unpaarer Primzahlen $r, s \ldots$ oder auch das Produkt von Potenzen solcher Primzahlen, also $q = r^m s^n \ldots$ ist; so ist D dann, aber auch nur dann ein quadratischer Rest nach q, wenn es ein solcher nach jedem einzelnen der Primfaktoren $r, s \ldots$ ist, wenn man also hat

(4) $$D^{\frac{r-1}{2}} \equiv 1 \mod r, \quad D^{\frac{s-1}{2}} \equiv 1 \mod s \quad \text{u. s. w.}$$

Denn zuvörderst leuchtet aus dem Satze II. ein, dass D dann und auch nur dann quadratischen Rest resp. nach r^m, $s^n \ldots$ ist,

wenn es ein solcher nach r, s... ist, wenn also die Bedingungen (4) erfüllt sind. Wenn aber

$$D \equiv x^2 \, mod \, r^m, \quad D \equiv y^2 \, mod \, s^n \text{ u. s. w.}$$

ist; so hat man die Gleichungen

$$D - x^2 = vr^m$$
$$D - y^2 = ws^n$$
u. s. w.

und demnach auch

$$D - (x + v'r^m)^2 = D - x^2 - 2v'xr^m - v'^2r^{2m} = (v - 2v'x - v'^2r^m)r^m$$
$$D - (y + w's^n)^2 = D - y^2 - 2w'ys^n - w'^2s^{2n} = (w - 2w'y - w'^2s^n)s^n$$
u. s. w.

In diesen Gleichungen bezeichnen die Buchstaben v, w... gewisse und die Buchstaben v', w'... ganz willkürliche ganze Zahlen. Da von den Grössen r^m, s^n... keine zwei ein gemeinschaftliches Maass haben; so können die Zahlen v', w'... so bestimmt werden, dass

$$x + v'r^m = y + w's^n = \text{etc.}$$

ist. (S. den zweiten Abschnitt.) Alsdann erhält man aber

$$D - (x + v'r^m)^2 = D - (y + w's^n)^2 = \text{etc.} \quad \text{oder}$$
$$D - X^2 = D - Y^2 = \text{etc.}$$

Da nun der erste, zweite etc. dieser einander gleichen Ausdrücke resp. durch r^m, s^n etc. theilbar ist und diese Theiler relativ prim sind; so folgt, dass es einen Werth für X gibt, wodurch $D - X^2$ durch das Produkt $r^m s^n \ldots = q$ theilbar wird, dass also D ein quadratischer Rest nach q ist, sobald es ein solcher nach jeder der Zahlen r, s... ist.

Dass umgekehrt, wenn D kein quadratischer Rest nach irgend Einer der Zahlen r, s... ist, es auch kein solcher nach $q = r^m$, s^n... sein kann, leuchtet von selbst ein.

B. Wenn q eine Potenz von 2, aber relativ prim zu D ist.

IV. Wenn $q = 2$; so ist jeder paare oder unpaare Werth von D quadratischer Rest nach q. Es ist also allgemein

(5) $$D \equiv x^2 \, mod \, 2$$

Denn ist D paar $= 2r$; so hat man

$$2r = (2v)^2 + 2w, \quad \text{also} \quad \equiv (2v)^2 \, mod \, 2$$

Ist dagegen D unpaar $= 2r + 1$; so hat man

$$2r + 1 = (2v + 1)^2 + 2w, \quad \text{also} \quad \equiv (w + 1)^2 \, mod \, 2$$

Man kann in diesen Formeln stets v willkürlich annehmen und danach w angemessen bestimmen.

V. Wenn $q = 2^2 = 4$, und D relativ prim zu q, also unpaar; so ist jeder Werth D von der Form $4r + 1$

quadratischer Rest und jeder Werth D von der Form $4r+3$ quadratischer Nichtrest nach q. Es ist also

(6) $$4r+1 \equiv x^2 \bmod 4$$

(7) $$4r+3 \text{ nicht } \equiv x^2 \bmod 4$$

Denn es ist

$$4r+1=(2v+1)^2+4w, \text{ also } \equiv (2v+1)^2 \bmod 4$$

Dagegen kann $4r+3$ weder $=(2v)^2+4w$, noch $=(2v+1)^2+4w$, also überhaupt nicht $=x^2+4w$ oder $\equiv x^2 \bmod 4$ sein.

In allen diesen Formeln kann, wenn D negativ ist, r negativ gedacht werden. So hat man z. B. für $D=-1$ die Form $D=-4+3=4r+3$; also ist -1 ein quadratischer Nichtrest nach 4.

VI. Wenn $q=2^n$, worin $n>2$ ist, und D relativ prim zu q, also unpaar; so ist jeder Werth D von der Form $8r+1$ quadratischer Rest, dagegen jeder Werth D von der Form $8r+3$, $8r+5$, $8r+7$ quadratischer Nichtrest nach q. Es ist also

(8) $$8r+1 \equiv x^2 \bmod 2^n$$

(9) $$\left.\begin{matrix} 8r+3 \\ 8r+5 \\ 8r+7 \end{matrix}\right\} \text{ nicht } \equiv x^2 \bmod 2^n$$

Denn zuvörderst erhellet für $n=3$, also für $q=2^3=8$, dass

$$8r+1=(4v+1)^2+8w, \text{ also } \equiv (4v+1)^2 \bmod 8$$

ist, wodurch die Formel (8) für $n=3$ erwiesen ist.

Wenn man nun gefunden hätte, dass für irgend eine Potenz 2^n von 2, welche höher ist, als die zweite,

$$8r+1 \equiv x^2 \bmod 2^n, \text{ also } 8r+1-x^2=v2^n$$

wäre, worin x nothwendig eine unpaare Zahl sein müsste; so würde für eine willkürliche ganze Zahl w

$$\begin{aligned} 8r+1-(x+w2^{n-1})^2 &= 8r+1-x^2-wx2^n-w^2 2^{2n-2} \\ &= v2^n-wx2^n-w^2 2^{2n-2} \\ &= (v-wx-w^2 2^{n-2})2^n \end{aligned}$$

sein. Da aber x unpaar ist; so kann man die willkürliche Zahl w stets so wählen, dass $v-wx$ paar, also $=2u$, mithin

$$8r+1-(x+w2^{n-1})^2=(u-w^2 2^{n-3})2^{n+1}$$

folglich

$$8r+1 \equiv (x+w2^{n-1})^2 \bmod 2^{n+1}$$

wird.

Da nun bereits nachgewiesen, dass jeder Werth D von der Form $8r+1$ ein quadratischer Rest nach $q=2^3$ ist; so folgt aus dem letzteren Satze, dass er es auch nach jeder höheren Potenz 2^4, 2^5, 2^6... von 2 sein wird, womit die Beziehung (8) erwiesen ist.

Was dagegen die übrigen unpaaren Werthe D von der Form $8r+3$, $8r+5$, $8r+7$ betrifft; so kann offenbar keiner derselben $=(2v)^2+w2^n$ sein, weil der letztere Werth paar ist. Er kann aber auch nicht $=(2v+1)^2+w2^n=4v(v+1)+1+8w2^{n-3}$ sein, wenn $n>2$, also $w2^n=8w2^{n-3}$ ist, man mag v als paar oder als unpaar voraussetzen, weil der letztere Werth stets die Form $8r+1$ hat. Demnach kann keiner dieser Werthe von $D=x^2+w2^n$ oder $\equiv x^2 \, mod \, 2^n$ sein, womit die Beziehungen (9) erwiesen sind.

In allen vorstehenden Formeln kann, wenn D negativ ist, r negativ gedacht werden. So hat man z. B. für $D=-1$ die Form $D=-8+7=8r+7$; also ist -1 ein quadratischer Nichtrest nach 2^n.

C Wenn q die Potenz einer in D aufgehenden Primzahl ist.

VII. Wenn q in D aufgeht; so ist D stets ein quadratischer Rest nach q, welchen Werth auch q haben möge.

Dieser Satz leuchtet von selbst ein.

VIII. Wenn q in D nicht aufgeht, aber die Potenz einer in D aufgehenden Primzahl r (welche auch $=2$ sein kann) darstellt, wenn man also $q=r^m$ und $D=r^nD'$ hat, worin $m>n$ ist und der Faktor D' die Primzahl r nicht weiter enthält; so ist D ein quadratischer Nichtrest nach q, wenn n einen unpaaren Werth hat.

Denn wäre $D\equiv x^2 \, mod \, r^m$, also

$$r^nD' = x^2 + vr^m$$

so müsste, da r^m durch r^n theilbar ist, auch x^2 durch r^n theilbar sein. Da aber r eine Primzahl und r^n eine unpaare Potenz davon ist; so müsste x^2 auch durch die paare Potenz r^{n+1} theilbar sein, folglich die Form y^2r^{n+1} haben. Dividirt man also die vorstehende Gleichung durch r^n; so müsste sich eine Gleichung von der Form

$$D' = y^2r + vr^{m-n} = (y^2 + vr^{m-n-1})r$$

ergeben. Hiernach müsste D' durch r theilbar sein, was der Voraussetzung widerspricht.

IX. Hat dagegen für die vorstehende Voraussetzung n einen paaren Werth; so ist D ein quadratischer Rest oder Nichtrest nach q, jenachdem D' ein quadratischer Rest oder Nichtrest nach r ist.

Denn wenn $D\equiv x^2 \, mod \, r^m$ oder

$$r^nD' = x^2 + vr^m.$$

sein soll; so muss, da r^m durch r^n theilbar ist, auch x^2 durch r^n theilbar sein. Da aber r^n eine paare Potenz ist; so muss x^2 die Form y^2r^n haben; es muss also, wenn man die vorstehende Gleichung durch r^n dividirt,

$$D' = y^2 - vr^{m-n} = y^2 + vr^{m-n-1}r$$

d. h. es muss

$$D' \equiv y^2 \bmod r$$

sein. Damit also D ein quadratischer Rest nach q sei, muss D' ein solcher nach r sein. (Das Letztere ist stets der Fall für $D' = 1$.)

Auf demselben Wege ergibt sich auch leicht der umgekehrte Satz, dass nämlich, damit D ein quadratischer Nichtrest nach q sei, auch D' ein solcher nach r sein müsse.

D. Allgemeiner Fall, wo q in beliebiger Weise zusammengesetzt ist.

X. Ist endlich für den allgemeinsten Fall q das Produkt aus beliebigen Primzahlen oder Potenzen derselben, also von der Form $r^m s^n \ldots$, worin die Primzahlen $r, s \ldots$ an keine Einschränkung gebunden sind; so führt eine Betrachtung ähnlich der sub III. zu dem Schlusse, dass D dann und auch nur dann ein quadratischer Rest nach q sei, wenn es ein solcher nach jeder der Zahlen $r^m, s^n \ldots$ ist. Auf die letztere Eigenschaft kann aber D jederzeit durch die betreffenden der vorstehenden Sätze geprüft werden.

Wir machen noch darauf aufmerksam, dass wenn r, s irgend zwei zusammengesetzte, aber relativ prime Zahlen sind, und es ist D ein quadratischer Rest sowol nach r, wie nach s, stets auch D ein quadratischer Rest nach dem Produkte rs sein wird.

XI. Von besonderer Wichtigkeit ist es übrigens, dass wenn D und q ein gemeinschaftliches Maass haben, die Untersuchung stets auf den einfacheren Fall zurückgeführt werden kann, wo beide Zahlen relativ prim sind, und zwar auf folgende Weise.

Besitzen D und q irgend ein Quadrat als gemeinschaftlichen Faktor, ist also $D = a^2D'$ und $q = a^2q'$; so kann dasselbe aus beiden Zahlen ohne Weiteres entfernt werden, sodass also D quadratischer Rest oder Nichtrest nach q ist, wenn D' ein solcher nach q' ist.

Denn wenn $a^2D' = x^2 + va^2q'$ sein soll; so muss x^2 durch a^2, also x durch a theilbar, folglich $x = ax'$, also auch $D' = x'^2 + vq'$ d. h. es muss D' ein quadratischer Rest nach q' sein. Werden nun durch Beseitigung der gemeinschaftlichen Quadrate aus D und q beide Zahlen relativ prim; so hat man

das gewünschte Ziel erreicht. Behalten jedoch hiernach D und q noch ein gemeinschaftliches Maass; so kann dasselbe nur aus den ersten Potenzen verschiedener Primzahlen, also nur von der Form $rs\ldots$ sein. Einen jeden Faktor r, $s\ldots$ dieses gemeinschaftlichen Maasses berücksichtigen wir nun besonders, und zwar in nachstehender Art.

Kommt der gemeinschaftliche Primfaktor r nur Einmal in q und Ein oder mehr Mal in D vor, hat man also $q = rq'$ und $D = rD'$ oder $= r^n D'$; so kann derselbe in q gestrichen werden, sodass also D ein quadratischer Rest oder Nichtrest nach q ist, jenachdem es ein solcher nach q' ist.

Denn nach dem Satze X. wird verlangt, dass die Zahl D, wenn sie quadratischer Rest nach q sein soll, gleichzeitig ein solcher Rest nach r und auch nach q' sein müsse. Da aber r in D aufgeht; so ist nach dem Satze VII. die erste Bedingung, dass D ein quadratischer Rest nach r sei, unbedingt erfüllt, und es kommt nur noch auf die zweite an, ob D ein solcher Rest nach q' sei.

Kommt dagegen der Primfaktor r nur Einmal in D, dagegen mehr als Ein Mal in q vor, hat man also $D = rD'$ und $q = r^n q'$; so ist nach dem Satze VIII. sofort zu schliessen, dass D ein quadratischer Nichtrest nach q sei.

Berücksichtigt man auf diese Weise jeden einzelnen Faktor des etwa noch zurückgebliebenen gemeinschaftlichen Maasses $rs\ldots$; so gelangt man entweder zu dem Schlusse, dass D ein quadratischer Nichtrest nach q sei, oder man erhält zur weiteren Untersuchung zwei relativ prime Zahlen.

Im Allgemeinen ist klar, dass wenn irgend ein Primfaktor, welcher den beiden Zahlen D und q gemeinschaftlich angehört und in D auf unpaarer Potenz erscheint, in q auf höherer Potenz, als in D vorkommt, D jedenfalls ein quadratischer Nichtrest nach q ist.

XII. Nachdem auf diese Weise D und q relativ prim gemacht sind, lässt sich die Rechnung oftmals auf noch kleinere Zahlen bringen.

Wenn nämlich D einen quadratischen Faktor enthält, also $D = a^2 D'$ ist, kann derselbe ohne Weiteres herausgeworfen werden, sodass also D ein quadratischer Rest oder Nichtrest nach q ist, wenn D' ein solcher nach q ist.

Denn wenn

$$a^2 D' = x^2 + vq \qquad \text{so ist auch}$$
$$a^2 D' = (x + v'q)^2 + wq$$

Da nun a und q relativ prim sind; so kann man stets zwei ganze Zahlen v' und y bestimmen, für welche $x + v'q = ay$ also

$$a^2 D' = a^2 y^2 + wq$$

wird. In dieser Gleichung muss offenbar das letzte Glied wq durch a^2 theilbar sein: da aber a und q relativ prim sind; so muss der Faktor w allein durch a^2 theilbar sein. Man muss also haben, wenn man mit a^2 dividirt, $D' = y^2 + w'q$, d. h. D' muss ein quadratischer Rest nach q sein.

Eine fernere Vereinfachung ist thunlich, wenn der Model q paar ist, aber den Faktor 2 nur auf erster Potenz enthält, wenn also $q = 2q'$ und q' unpaar ist. In diesem Falle kann man den Faktor 2 ohne Weiteres aus dem Werthe von q herausstossen, sodass also D ein quadratischer Rest nach q ist, wenn es ein solcher nach q' ist.

Dies erhellet aus dem Satze X., wonach, wenn D quadratischer Rest nach $q = 2q'$ sein soll, es ein solcher Rest sowol nach 2, als auch nach q' sein muss. Die erstere Bedingung ist aber nach dem Satze IV. jederzeit erfüllt; es kommt also nur noch auf die zweite an.

XIII. Endlich machen wir noch darauf aufmerksam, dass wenn D numerisch grösser als q sein sollte, man für D stets seinen kleinsten positiven Rest nach q nehmen kann, welcher immer kleiner als q sein wird.

Wenn man will, kann man die Zahl D sogar dann noch verkleinern, wenn dieselbe numerisch grösser als $\frac{q}{2}$ ist, indem man für D seinen absolut kleinsten Rest nach q nimmt, welcher bald positiv, bald negativ, jedoch numerisch stets $\leqq \frac{q}{2}$ ist.

Denn es leuchtet ein, dass wenn $D = vq + D'$ ist, D ein quadratischer Rest oder Nichtrest nach q ist, wenn D' ein solcher ist.

XIV. Beispiele. Um zu entscheiden, ob $D = 2^2 . 3^3 . 5^5 . 7$ quadratischer Rest nach $q = 2^3 . 3^3 . 5 . 11$ sei, kann man erst in D und q den gemeinschaftlichen quadratischen Faktor $2^2 . 3^2$ streichen. Hierdurch reduzirt sich die Frage darauf, ob $(3 . 5^5 . 7) R (2 . 3 . 5 . 11)$ sei. Jetzt kann in q der Faktor 2, alsdann aber auch jeder der beiden in D enthaltenen Primfaktoren 3 und 5 gestrichen werden, wonach die Frage $(3 . 5^5 . 7) R 11$ zu entscheiden ist. Hierauf kann D von dem quadratischen Faktor 5^4 befreiet werden. Dies reduzirt die Aufgabe auf die Frage $(3 . 5 . 7) R 11$ oder $105 R 11$ oder wenn man jetzt für 105 seinen kleinsten positiven Rest nach 11 nimmt, auf die Frage $6 R 11$,

welche sich sehr leicht dahin entscheidet, dass 6 kein quadratischer Rest nach 11, dass vielmehr $6N11$ sei. Demnach ist auch $2^2.3^3.5^5.7$ kein quadratischer Rest nach $2^4.3^3.5.11$.

Die Frage, ob $D=3^3.13$ quadratischer Rest nach $q=3^4.19$ sei, ist nach dem Satze XI. sofort zu verneinen, weil der gemeinschaftliche Primfaktor 3, welcher in D auf unpaarer Potenz erscheint, in q auf höherer Potenz vorkommt, als in D.

Um zu untersuchen, ob $2^2.5^2.13$ ein quadratischer Rest nach $2^4.5^2.13$ sei, kann man den gemeinschaftlichen Faktor $2^2.5^2$ aus D und q und den Faktor 13 aus q entfernen. Dies gibt die Frage $13R2^2$ oder $13R4$, welche bejahet werden muss. Demnach ist $2^2.5^2.13$ ein quadratischer Rest nach $2^4.5^2.13$.

§. 151. Berücksichtigung der Faktoren eines quadratischen Restes.

I. In dem vorhergehenden Paragraphen hat sich zur Beurtheilung, ob D ein quadratischer Rest nach q sei, die Kenntniss der Primfaktoren des Models q, nicht aber die der Zahl D als nothwendig erwiesen. Sind jedoch Faktoren bekannt, deren Produkt gleich D ist (wobei es gleichgültig bleibt, ob jene Faktoren prim sind oder nicht); so kann die Untersuchung, ob D ein quadratischer Rest nach q sei, auf die Untersuchung, wie viel jener Faktoren quadratische Reste und wie viel derselben quadratische Nichtreste nach q (resp. nach den Faktoren von q) sind, zurückgeführt werden.

Die beiden Fälle, wo $q=2$ oder wo q in D aufgeht, bedürfen keiner weiteren Berücksichtigung, da in diesen beiden Fällen D stets ein quadratischer Rest nach q ist.

Was die übrigen Fälle betrifft; so betrachten wir erst den, wo q eine Primzahl ist. Hierfür haben wir folgenden Lehrsatz.

Von den Faktoren, deren Produkt $=D$ ist, sind etliche quadratische Reste und die übrigen quadratische Nichtreste nach q. Ist die Anzahl der **Nichtreste paar** (oder auch gleich **null**); so ist D quadratischer **Rest**: ist dieselbe dagegen **unpaar**; so ist D quadratischer **Nichtrest** nach q.

Denn damit D ein quadratischer Rest oder Nichtrest nach q sei, muss $D^{\frac{q-1}{2}}$ resp. $\equiv 1$ oder $\equiv -1 \mod q$ oder es muss, wenn man den kleinsten Rest von $D^{\frac{q-1}{2}}$ nach dem Model q in der Legendreschen Weise mit $\left(\frac{D}{q}\right)$ bezeichnet, $\left(\frac{D}{q}\right)$ resp. $=1$ oder $=-1$ sein.

Ist nun D auf irgend eine Weise in die Faktoren $a, b, c\ldots$ zerlegt (welche nicht nothwendig prim zu sein brauchen), hat man also $D = abc\ldots$; so ist offenbar

$$\left(\frac{D}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)\left(\frac{c}{q}\right)\ldots$$

und dieses Produkt ist nur dann $= 1$, wenn von den Faktoren $\left(\frac{a}{q}\right), \left(\frac{b}{q}\right), \left(\frac{c}{q}\right)$ gar keiner oder eine paare Menge $= -1$ sind. Dagegen ist jenes Produkt $= -1$, wenn von den letzteren Faktoren eine unpaare Menge $= -1$ sind.

II. Hieraus erkennt man nochmals, wie in §. 150, XII., dass wenn D einen quadratischen Faktor a^2 enthält, derselbe unberücksichtigt bleiben, also ohne Weiteres ausgestossen werden kann, indem $\left(\frac{a^2}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{a}{q}\right)$ in allen Fällen $= 1$ ist.

III. Ferner kann man, wie bereits in §. 150, XIII. erwähnt, wenn D numerisch grösser als q ist, für D seinen kleinsten positiven Rest nach dem Model q, welcher kleiner als q ist, oder auch, wenn D grösser als $\frac{q}{2}$ ist, seinen absolut kleinsten Rest, welcher numerisch kleiner als $\frac{q}{2}$ aber bald positiv, bald negativ ist, setzen.

IV. Bringt man die vorstehenden Betrachtungen mit dem Reziprozitätsgesetze (§. 148, IX., X.) in Verbindung; so ergibt sich das folgende, oftmals sehr bequeme Verfahren zur Untersuchung, ob D ein quadratischer Rest nach q sei oder nicht.

Nachdem man D (oder seinen sub III. genannten kleinsten Rest) von seinen quadratischen Faktoren befreiet und, was übrig bleibt, in seine Primfaktoren $a, b, c\ldots$ zerlegt hat, reduzirt sich die Untersuchung darauf, welche der Ausdrücke $\left(\frac{a}{q}\right), \left(\frac{b}{q}\right), \left(\frac{c}{q}\right)$ gleich $+1$ und welche gleich -1 seien.

Ist Einer der Faktoren $a, b, c\ldots$ gleich ± 2; so entscheidet sich, ob $\left(\frac{\pm 2}{q}\right) = 1$ oder $= -1$ sei, je nach der Form von q durch §. 148, XIII., XIV.

Jeden anderen der Ausdrücke $\left(\frac{a}{q}\right), \left(\frac{b}{q}\right), \left(\frac{c}{q}\right)\ldots$, wie z. B. $\left(\frac{a}{q}\right)$, worin jetzt unbedingt der absolute Werth

von r kleiner als q sein wird, kann man nun mit Hülfe des Reziprozitätsgesetzes, §. 148, IX., X., umkehren, sodass die grössere Zahl q in den Zähler und die kleinere r in den Nenner tritt, indem man nach jenem Gesetze stets $\left(\frac{a}{q}\right)=\pm\left(\frac{q}{a}\right)$ hat.

Nach dieser Umkehrung nimmt man statt jedes Zählers dessen kleinsten Rest in Beziehung zu dem betreffenden Nenner, wie man es sub III. bereits mit dem Ausdrucke $\left(\frac{D}{q}\right)$ gethan hatte, und operirt mit jedem einzelnen der so erhaltenen Ausdrücke in der vorstehend beschriebenen Weise weiter.

So oft man auf einen quadratischen Rest oder auf zwei quadratische Nichtreste trifft; stösst man dieselben aus der ferneren Rechnung heraus. Endlich aber muss man, da sich die Zähler der fraglichen Ausdrücke immer verkleinern, auf lauter Ausdrücke stossen, welche entweder $+2$ oder $+1$ zum Zähler haben, und demnach nach §. 148, XIII. bis XV. bestimmt werden können.

V. Beispiel. Um zu ermitteln, ob die Zahl 2039 quadratischer Rest oder Nichtrest nach der Primzahl 787 sei, ob es also Zahlen von der Form $2039-x^2$ gebe, welche durch 787 theilbar sind, setzen wir, da zuvörderst eine Division mit 787 in 2039 den Rest 465 gibt,

$$\left(\frac{2039}{787}\right)=\left(\frac{465}{787}\right)=\left(\frac{3.5.31}{787}\right)=\left(\frac{3}{787}\right)\left(\frac{5}{787}\right)\left(\frac{31}{787}\right)$$

also nach dem Reziprozitätsgesetze

$$=-\left(\frac{787}{3}\right).\left(\frac{787}{5}\right).-\left(\frac{787}{31}\right)=\left(\frac{787}{3}\right)\left(\frac{787}{5}\right)\left(\frac{787}{31}\right)$$

oder wenn man mit den Nennern dividirt,

$$=\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)\left(\frac{23}{31}\right)\text{d.i. nach §. } 148=1.-1.-\left(\frac{31}{23}\right)=\left(\frac{31}{23}\right)$$

und wenn man jetzt nochmals mit dem Nenner dividirt, $=\left(\frac{8}{23}\right)=\left(\frac{2^2.2}{23}\right)$, also wenn man den quadratischen Faktor 2^2 ausser Acht lässt, $=\left(\frac{2}{23}\right)$ d. i. nach §. 148 $=1$. Dies lehrt, dass 2039 quadratischer Rest nach 787 sei.

VI. Gehen wir jetzt zu den allgemeineren Fällen mit zusammengesetztem Model über.

Wenn der Model q eine zusammengesetzte, aber zu D relativ prime Zahl von der Form $2^v r^m s^n \ldots$ ist, worin

r, s verschiedene unpaare Primzahlen bezeichnen; so hat man einzeln zu untersuchen, wie viel der Faktoren a, b..., welche das Produkt D bilden, quadratische Reste, und wie viel derselben quadratische Nichtreste nach dem Faktor 2^v und nach jedem einzelnen der unpaaren Primfaktoren r, s... sind.

Ist die Anzahl der **Nichtreste** sowol nach 2^v, als auch nach jedem einzelnen der unpaaren Primfaktoren r, s... **paar**; so ist D ein quadratischer Rest nach q; im entgegengesetzten Falle aber ein **Nichtrest.**

Denn nach §. 150, X. und III. kann die Zahl $D = ab\ldots$ nur dann ein quadratischer Rest nach $q = 2^v r^m s^n \ldots$ sein, wenn sie ein solcher nach jeder der Zahlen 2^v, r, s... ist.

Betrachten wir erst die unpaaren Primzahlen r, s.... Ist a ein quadratischer Rest nach r; so hat man $\left(\frac{a}{r}\right) = 1$.

Ist dagegen b ein quadratischer Nichtrest nach r; so hat man $\left(\frac{b}{r}\right) = -1$.

Ist nun die Anzahl dieser Nichtreste $= w$; so ergibt sich durch Multiplikation aller nach dem Model r gebildeten Ausdrücke wie $\left(\frac{a}{r}\right)$, $\left(\frac{b}{r}\right)$...

$$\left(\frac{D}{r}\right) = \left(\frac{a}{r}\right)\left(\frac{b}{r}\right)\ldots = (-1)^w$$

Damit also D quadratischer Rest nach r sein könne, muss nothwendig w paar sein.

Dieselbe Beziehung muss für s und die übrigen unpaaren Primfaktoren von q, wenn dieselben als Model angenommen werden, stattfinden.

Was nun die in dem Model q etwa enthaltene Potenz 2^v der paaren Primzahl 2 betrifft; so ergibt sich hierfür der Beweis des obigen Satzes folgendermaassen.

Ist der Faktor 2 nur auf erster Potenz vorhanden, also $v = 1$; so gibt es unter den Zahlen a, b... keine, also null, d. i. eine paare Menge quadratischer Nichtreste nach 2. Jetzt ist auch D stets ein quadratischer Rest nach 2. Der obige Satz ist also auch für diesen Fall gültig; man erkennt übrigens, dass es jetzt nur auf das Verhalten der übrigen Faktoren von q ankommt, und dass man den Faktor 2 von q ganz ausstossen kann.

Ist der Faktor 2 auf zweiter Potenz vorhanden, also $v = 2$ und $2^v = 4$; so geht aus §. 150, V. hervor, dass die unter den Zahlen a, b... vorkommenden quadratischen Reste nach 4 die Form $4n + 1$, die Nichtreste dagegen die Form $4n + 3$ haben.

Das Produkt aus beliebig vielen Faktoren der ersteren Form $4n+1$ behält immer dieselbe Form, bleibt also stets ein quadratischer Rest nach 4. Dagegen nimmt das Produkt aus einer paaren Menge von Faktoren der letzteren Form $4n+3$ die erstere Form $4n+1$ an, wird also zu einem quadratischen Reste nach 4; das Produkt aus einer unpaaren Menge von Faktoren jener letzteren Form $4n+3$ behält aber dieselbe Form $4n+3$, bleibt also ein quadratischer Nichtrest nach 4. Demnach muss, damit D ein quadratischer Rest nach 4 sein könne, unter den Faktoren $a, b \ldots$ eine paare Menge quadratischer Nichtreste nach 4 vorkommen, wie es der obige Lehrsatz verlangt.

Ebenso schliesst man, wenn der Faktor 2 auf dritter oder noch höherer Potenz vorhanden, also $v>2$ ist, indem man nach §. 150, VI. beachtet, dass dann $4n+1$ die Form der quadratischen Reste und $4n+3$, $4n+5$, $4n+7$ die Formen der quadratischen Nichtreste nach 2^v sind.

Im Uebrigen hat man zur Entscheidung, ob D ein quadratischer Rest nach 2^v sei, nicht nöthig, D erst in Faktoren $a, b \ldots$ zu zerlegen, indem dieser Umstand nach §. 150, V., VI. sofort aus der Form von D geschlossen werden kann.

Auch in dem vorstehenden Falle ist nach §. 150, XII. klar, dass man jeden quadratischen Faktor aus dem Werthe von D entfernen kann.

VII. Wenn der Model q mit D ein gemeinschaftliches Maass besitzt; so kann der Fall nach §. 150, XI. leicht auf den vorhergehenden, wo q und D relativ prim sind, auch D keinen quadratischen Faktor enthält, zurückgeführt werden, wenn nicht irgend ein gemeinschaftlicher und in D auf unpaarer Potenz erscheinender Primfaktor öfter in q, als in D vorkommt, also sofort erkannt wird, dass D ein quadratischer Nichtrest nach q sei.

Nachdem Dies geschehen, kann man die Frage, ob D ein quadratischer Rest nach q, ob also DRq sei, folgendermaassen auf die einfachsten Rechnungen zurückführen. Es sei $D=\pm abc\ldots$ worin $a, b, c\ldots$ lauter verschiedene Primzahlen darstellen, von denen Eine, wenn D negativ ist, negativ sein wird. Ferner sei $q=2^v r^m s^n\ldots$, worin $r, s\ldots$ verschiedene Primzahlen darstellen. Damit nun DRq sei, wird entweder erfordert, dass

$$DR2^v$$
$$aRr, \quad bRr, \quad cRr\ldots$$
$$aRs, \quad bRs, \quad cRs\ldots$$
u. s. w.

sei, oder doch, dass in jeder der vorstehenden Horizontalreihen, von der zweiten an gerechnet, nur eine paare Menge von Nichtresten vorkomme.

§. 152. Auflösung der quadratischen Kongruenzen. — Anzahl der Wurzeln.

I. Durch die Lehren der vorstehenden Paragraphen kann man leicht entscheiden, ob eine gegebene Zahl D ein quadratischer Rest oder Nichtrest nach einer anderen gegebenen Zahl q, ob also die reine quadratische Kongruenz

(1) $$D \equiv x^2 \mod q$$

möglich sei oder nicht, oder ob es Zahlen von der Form $D - x^2$ gebe, welche durch q theilbar seien, ein Umstand, dessen Wichtigkeit für die unbestimmten Gleichungen vom zweiten Grade man bereits zu würdigen gelernt hat.

Die Werthe der Wurzeln x selbst, für welche die Kongruenz (1) erfüllt wird, ergeben sich jedoch durch jene Untersuchungen nicht. Um dieselben zu finden, kann man sich der Methode des §. 77 und 78 bedienen, welche an sich einfach und von dem Werthe des Models q ganz unabhängig ist, auch nach §. 79 für den Fall, dass die Faktoren von q bekannt sind, noch weiter abgekürzt werden kann.

Wollte man die Wurzeln x im eigentlichen Sinne der Kongruenzenrechnung bestimmen; so würde Dies eine der Methode in §. 76 ähnliche Rechnung nach sich ziehen. Man hätte dann zuvörderst für D seinen kleinsten positiven Rest nach dem Model q zu substituiren, also wenn derselbe mit D' bezeichnet wird, statt der Formel (1) die folgende zu nehmen

(2) $$D' \equiv x^2 \mod q$$

Bildet man jetzt die kleinsten positiven Reste der Quadrate der natürlichen Zahlen $x = 0, 1, 2, 3 \ldots$, also die Reste von $x^2 = 0, 1, 4, 9 \ldots$, wobei x nicht grösser, als $\frac{q}{2}$ genommen zu werden braucht; so liefert jeder Werth von x eine gesuchte Wurzel, dessen Quadrat einen Rest $= D'$ ergibt.

Jeder auf diese Weise für x gefundene Werth p kann sowol positiv, wie negativ genommen werden und repräsentirt demnach zwei verschiedene Auflösungen $\pm p$, welche numerisch $\leqq \frac{q}{2}$ sind und nur dann wie eine einzige zu betrachten sind, wenn entweder $p = 0$ oder wenn $p = \frac{q}{2}$ ist. Alle diese Werthe von $\pm p$ zusammengenommen stellen die absolut kleinsten Wurzeln dar.

Nimmt man von je zwei Werthen wie $\pm p$ den positiven Werth $+p$ und anstatt des negativen Werthes $-p$ den gleichfalls positiven Werth $q - p$; so erhält man zwei zusammengehörige Auflösungen p und $q - p$, welche beide positiv und

$< q$ sind. Alle diese Werthe zusammengenommen, stellen die kleinsten positiven Wurzeln dar.

Jede einzelne dieser Wurzeln ist das Glied einer unendlichen Reihe von Werthen für x, welche sämmtlich die Kongruenz (1) erfüllen. Alle Glieder einer solchen Reihe sind aber einander nach dem Model q kongruent, indem man, wenn p irgend Eine der vorstehend genannten kleinsten Wurzeln ist, allgemein

(3) $$x = p + vq \quad \text{oder} \quad x \equiv p \bmod q$$

hat, worin v jede beliebige ganze Zahl bedeutet.

Wir bemerken noch, dass Gauss die Wurzel der Kongruenz (1), ähnlich wie bei den Gleichungen durch das Symbol $\sqrt{D} \bmod q$ andeutet, sodass man allgemein $x \equiv \sqrt{D} \bmod q$ hat.

II. Die nach dem Obigen erforderliche Bildung der Reste der Quadrate 0, 1, 4, 9... erleichtert sich durch die Bemerkung, dass die späteren Quadrate aus dem unmittelbar vorhergehenden durch Hinzufügung resp. der unpaaren Zahlen 1, 3, 5... entstehen, indem man hat

x	$2x+1$	x^2
0	1	0
1	3	$1 = 0 + 1$
2	5	$4 = 1 + 3$
3	7	$9 = 4 + 5$
4		$16 = 9 + 7$

etc.

Demnach braucht man, um die Reste von 0, 1, 4, 9... herzustellen, zu den bereits berechneten Resten nach und nach nur die Reste der unpaaren Zahlen 1, 3, 5... nach dem Model q hinzuzuaddiren, und von jeder sich ergebenden Summe, ehe man sie weiter durch Addition vermehrt, den kleinsten positiven Rest nach q zu nehmen.

III. Da in der Kongruenz (2) die Grösse D' den Rest von D nach dem Model q vertritt; so leuchtet ein, dass die Kongruenz (1) für alle Werthe von D, welche einander nach dem Model q kongruent sind, also für alle Werthe von der Form

(4) $$D = D' + vq$$

genau dieselben Wurzeln besitzt.

So hat man z. B. für den Model $q = 8$

$x = 0$	1	2	3	4
$x^2 = 0$	1	4	9	16
$\equiv 0$	1	4	1	0

Hieraus erkennt man, dass die Kongruenz (1) für jeden Werth von D, welcher $\equiv 0$ ist, also für $D = \ldots -16, \ -8,$

0, 8, 16 ... die drei absolut kleinsten Wurzeln $x = 0$, ± 4 besitzt, welche jedoch nur zwei verschiedene Wurzeln 0 und 4 enthalten, indem $+4$ und -4 nach dem Model 8 kongruent sind.

Für jeden Werth von D, welcher $\equiv 1$ ist, also für $D = \ldots -15, -7, 1, 9, 17 \ldots$ hat man die vier absolut kleinsten Wurzeln $x = \pm 1$, ± 3 oder die vier kleinsten positiven Wurzeln 1, 7, 3, 4.

Für jeden Werth von D, welcher $\equiv 4$ ist, also für $D = \ldots -12, -4, 4, 12, 20 \ldots$ hat man die beiden absolut kleinsten Wurzeln $x = \pm 2$ oder die beiden kleinsten positiven Wurzeln 2, 6.

Für jeden Werth D, welcher $\equiv 2, 3, 5$ oder 7 ist, gibt es keine Wurzel.

IV. Je kleiner der Model q, desto geringer ist der zur Auflösung der Kongruenz (1) erforderliche Rechenaufwand, wogegen die Grösse der Zahl D hierbei in der Regel gleichgültig ist. Demnach schafft es häufig bedeutende Vortheile, wenn man den Model q in Faktoren $q', q'', q''' \ldots$ zerlegt, von denen keine zwei ein gemeinschaftliches Maass besitzen, und hierauf erst jede der Kongruenzen

(5) $D \equiv x'^2 \bmod q', \quad D \equiv x''^2 \bmod q'', \quad D \equiv x'''^2 \bmod q''' \ldots$

auflös't. Ist dann resp. $p', p'', p''' \ldots$ eine Wurzel der ersten, zweiten, dritten ... Kongruenz; so hat man allgemein

(6) $x' = p' + v'q', \quad x'' = p'' + v''q'', \quad x''' = p''' + v'''q''' \ldots$

Diejenigen Werthe, für welche $x' = x'' = x''' = \ldots$ ist, liefern die gesuchten Wurzeln der Kongruenz (1). Für die Letzteren muss man also haben

(7) $x = p' + v'q' = p'' + v''q'' = p''' + v'''q''' = \ldots$

Da je zwei der Grössen $q', q'', q''' \ldots$ relativ prim sind; so ist jede Gleichung wie

(8) $p' + v'q' = p'' + v''q''$ oder $v'q' - v''q'' = p'' - p'$

in ganzen Zahlen für v' und v'' lösbar: es wird also immer Werthe für x geben, wenn es solche für $x', x'', x''' \ldots$ gibt.

Man erhält die positiven Werthe von x, welche $< q$ sind, sämmtlich, oder die Wurzeln der Kongruenz (1) vollständig, wenn man in den Gleichungen (7) alle positiven Werthe von $p', p'', p''' \ldots$, welche resp. $< q', q'', q''' \ldots$ sind, auf jede mögliche Weise mit einander kombinirt.

Fasst man zu diesem Ende erst die Eine Gleichung ins Auge, kombinirt man also erst alle Werthe von p' mit allen Werthen von p''; so ergeben sich die Wurzeln der Kongruenz $D \equiv y^2 \bmod q'q''$. Diese Wurzeln sind von der allgemeinen Form $y + wq'q''$. Setzt man also nun $y + wq'q'' = p''' + v'''q'''$, indem

man alle positiven Werthe von y, welche $< q'q''$ sind, mit allen Werthen von p''', welche $< q'''$ sind, kombinirt; so erhält man die Wurzeln der Kongruenz $D \equiv z^2 \, mod \, q'q''q'''$ u. s. w.

V. Aus der Gleichung (8) erhellet, dass die Kombination Eines positiven Werthes von p', welcher $< q'$ ist, mit Einem positiven Werthe von p'', welcher $< q''$ ist, immer nur einen einzigen positiven Werth von $x' = x''$ liefert, welcher $< q'q''$ ist. Denn eine Auflösung dieser Gleichung für v' und v'' ergibt, wenn a eine gewisse konstante, w aber eine willkürliche ganze Zahl darstellt, $v' = a + wq''$ also $x' = x'' = p' + aq' + wq'q''$. Alle hierdurch dargestellten Werthe von $x' = x''$ sind einander nach dem Model $q'q''$ kongruent; es ist also nur ein einziger darunter, welcher positiv und kleiner als $q'q''$ ist.

Gibt es also u' verschiedene positive Werthe für p', welche $< q'$ sind, oder u' verschiedene Wurzeln der Kongruenz $D \equiv x'^2 \, mod \, q'$, ferner u'' verschiedene Wurzeln der Kongruenz $D \equiv x''^2 \, mod \, q''$, ferner u''' verschiedene Wurzeln der Kongruenz $D \equiv x'''^2 \, mod \, q'''$ u. s. w.; so gibt es $u'u''$ Wurzeln der Kongruenz $D \equiv y^2 \, mod \, q'q''$, ferner $u'u''u'''$ Wurzeln der Kongruenz $D \equiv z^2 \, mod \, q'q''q'''$ u. s. w.

Der vorstehende Satz gibt das Mittel an die Hand, die Anzahl der Wurzeln der Kongruenz (1) für zusammengesetzte Model zu bestimmen. Es sind jedoch hierzu einige Spezialisirungen erforderlich, welche wir sogleich näher betrachten wollen.

VI. Wenn der Model q aus v unpaaren Primzahlen $r, s, t \ldots$ auf erster Potenz besteht, von denen keine in D aufgeht; so hat man $u' = u'' = u''' = \ldots = 2$. Die Kongruenz (1) besitzt also, wenn sie überhaupt möglich ist, 2^v Wurzeln.

VII. Wenn der Model $q = r^m$ die Potenz einer in D nicht enthaltenen unpaaren Primzahl r ist; so hat die Kongruenz (1), wenn sie überhaupt möglich ist, nur zwei Wurzeln.

Aus §. 150, II. weiss man, dass die Kongruenz $D \equiv x^2 \, mod \, r^m$ nur dann möglich ist, wenn die Kongruenz $D \equiv x^2 \, mod \, r$ es ist, und es leuchtet ein, dass die Auflösungen der ersteren auch die letztere erfüllen, jedoch nicht umgekehrt. Demnach kann man die letztere Kongruenz lösen und aus den allgemeinen Werthen ihrer Wurzeln, welche die Form $x = p + vr$ besitzen werden, diejenigen entnehmen, für welche $D - x^2$ durch r^m theilbar wird. Diese Werthe stellen dann die Wurzeln der ersten gegebenen Kongruenz dar.

Um darzuthun, dass sich auf diese Weise immer nicht mehr als zwei Wurzeln ergeben werden, wollen wir zeigen,

dass die Kongruenz $D \equiv x^2 \mod r^{m+1}$ nicht mehr Wurzeln hat, als die Kongruenz $D \equiv x^2 \mod r^m$. Zu diesem Ende beachten wir, dass alle Wurzeln der ersteren auch Wurzeln der letzteren sind, also unter diesen angetroffen werden müssen. Ist daher p eine spezielle und $p + wr^m$ die allgemeine Auflösung der letzteren Kongruenz; so hat man

$$D - p^2 = vr^m$$
$$D - (p + wr^m)^2 = (v - 2pw - w^2 r^m) r^m$$

Damit der letztere Ausdruck durch r^{m+1} theilbar werde, also $p + wr^m$ eine Wurzel der zuerst gegebenen Kongruenz darstelle, muss der Faktor von r^m auf der rechten Seite durch r, also auch $v - 2pw$ durch r theilbar sein. Man muss demnach

$$v - 2pw = ru \qquad \text{oder} \qquad ru + 2pw = v$$

haben. In dieser Gleichung wird p, also auch $2p$ die unpaare Primzahl r nicht enthalten; denn sonst müsste wegen der Gleichung $D - p^2 = vr^m$ auch r in D enthalten sein, was der Voraussetzung widerspricht. Wenn aber r und $2p$ relativ prim sind, ist die vorstehende Gleichung für u und w in ganzen Zahlen lösbar, und es wird sich w in der Form $a + w'r$ darstellen, worin a konstant und w' willkürlich ist. Durch diesen Ausdruck für w nimmt der Ausdruck $p + wr^m$, welcher nunmehr auch die Auflösung der ersten Kongruenz mit dem Model r^{m+1} darstellt, die Form $p + ar^m + w'r^{m+1}$ an. Alle hierdurch dargestellten Werthe sind einander nach dem Model r^{m+1} kongruent, demnach gibt es darunter nur einen einzigen, welcher positiv und kleiner als r^{m+1} ist.

Hieraus erhellet, dass jeder Werth von p oder jede Wurzel der Kongruenz vom Model r^m nur zu einer einzigen Wurzel der Kongruenz vom Model r^{m+1} führt, dass also die letztere Kongruenz nur so viel Wurzeln hat, als die erstere und dass mithin alle Kongruenzen von den Modeln $r, r^2, r^3 \dots$ nur zwei verschiedene Wurzeln besitzen.

VIII. Wenn der Model q eine Potenz der Primzahl 2 und zu D relativ prim (wenn also D unpaar ist) so hat die Kongruenz (1), wenn sie überhaupt möglich ist, jenachdem q die **erste** oder die **zweite** oder eine **höhere** Potenz von 2 darstellt, resp. 1 oder 2 oder 4 Wurzeln.

Denn zunächst erhellet, dass für $q = 2$ die fragliche Kongruenz, worin nach der Voraussetzung D unpaar ist, nur eine einzige Wurzel besitzt, welche durch Einen der beiden kongruenten Werthe $x = +1$ oder -1 dargestellt wird.

Für $q = 4$ muss D nach §. 150, V. die Form $4r + 1$ haben, wenn die Kongruenz überhaupt möglich sein soll, und man findet leicht, dass es jetzt zwei verschiedene Wurzeln, nämlich

in absolut kleinsten Zahlen $x \equiv +1$, -1, oder in kleinsten positiven Zahlen $x = 1$, 3, gibt.

Für $q = 8$ muss D nach §. 150, VI. die Form $8r + 1$ haben, wenn die Kongruenz möglich sein soll, und es ergibt sich leicht, dass alsdann vier verschiedene Wurzeln, nämlich in absolut kleinsten Zahlen $x = \pm 1$, ± 3, oder in kleinsten positiven Zahlen $x = 1$, 3, 5, 7, vorhanden sind.

Diese vier Wurzeln stehen für den Fall, dass $q = 8 = 2^3$ ist, in einer bemerkenswerthen Beziehung zu einander. Bezeichnet man nämlich irgend Eine derselben mit p; so können alle vier dargestellt werden durch p, $p + 4$, $-p$, $-p + 4$. Die Hälfte dieser Wurzeln, nämlich $x = 1$ und 3 gehören auch der vorhergehenden Kongruenz vom Model 4 an.

Um nun den obigen Satz in seiner Allgemeinheit zu beweisen, wollen wir zeigen, dass wenn für $n > 2$ die Kongruenz $D \equiv x^2 \, mod \, 2^n$ überhaupt vier Wurzeln besitzt, welche in der Beziehung p, $p + 2^{n-1}$, $-p$, $-p + 2^{n-1}$ zu einander stehen (wie es für $n = 3$ bereits gezeigt ist), auch die Kongruenz $D \equiv x^2 \, mod \, 2^{n+1}$ nur vier Wurzeln besitzt, welche in der analogen Beziehung zu einander stehen.

Offenbar ist jede Wurzel der zweiten Kongruenz vom Model 2^{n+1} auch eine Wurzel der ersten Kongruenz vom Model 2^n. Demnach müssen die allgemeinen Auflösungen der ersten alle Auflösungen der zweiten enthalten. Ist nun p irgend eine spezielle Auflösung, also $p + w2^n$ der allgemeine Ausdruck für die Auflösung der ersten Kongruenz; so muss dieser Ausdruck, wenn man darin für p nach und nach die vier Werthe p, $-p$, $p + 2^{n-1}$, $-p + 2^{n-1}$ setzt, und dann w variiren lässt, auf alle verschiedenen Wurzeln der zweiten Kongruenz hinführen.

Angenommen also, es sei p eine gemeinschaftliche Wurzel der beiden obigen Kongruenzen, so hat man

$$D - p^2 = v2^{n+1} \quad \text{und demnach auch}$$
$$D - (p + w2^n) = (v - wp - w^2 2^{n-1}) 2^{n+1}$$

Hieraus folgt, dass nicht bloss p, sondern allgemein $p + w2^n$, also jede nach dem Model 2^n zu p kongruente Wurzel der ersten Kongruenz auch eine Wurzel der zweiten Kongruenz vom Model 2^{n+1} darstellt. In diesem Ausdrucke sind jedoch nur zwei positive Werthe, welche kleiner als 2^{n+1} sind, also nur zwei verschiedene Wurzeln der zweiten Kongruenz enthalten, welche man einfach $= p$ und $p + 2^n$ setzen kann.

Nimmt man jetzt $-p$ für p; so findet sich, dass auch $-p$ und $-p + 2^n$ zwei Wurzeln der zweiten Kongruenz sind.

Dagegen kann weder $p + 2^{n-1}$, noch $-p + 2^{n-1}$ zu einer Auflösung der zweiten Kongruenz führen. Denn da nach der

Voraussetzung $D - p^2 = v2^{n+1}$ ist, worin offenbar p unpaar sein wird; so hat man

$$D - (\pm p + 2^{n-1} + w2^n)^2 = (2v \mp 2wp - w^2 2^n - w2^n - 2^{n-2} \mp p)2^n$$

ein Ausdruck, welcher nicht durch 2^{n+1} theilbar sein kann, da p unpaar ist.

Demnach hat die zweite Kongruenz nur vier Wurzeln, und dieselben können immer, welche derselben man auch mit p bezeichnen möge, durch p, $p + 2^n$, $-p$, $-p + 2^n$ dargestellt werden. Auch gehört die Hälfte derselben, nämlich die vorhin mit p und $-p$ bezeichneten, der ersten Kongruenz vom Model 2^n an.

IX. Wenn der Model q in D enthalten ist, aber aus lauter verschiedenen Primfaktoren besteht, also keinen quadratischen Faktor besitzt; so hat die Kongruenz (1) nur Eine Wurzel, nämlich $x = 0$.

Denn wenn in der Gleichung $D - x^2 = vq$ das erste Glied D durch q theilbar ist, und q keinen quadratischen Faktor enthält; so muss nicht bloss x^2, sondern x durch q theilbar, also entweder $= 0$ oder ein Vielfaches von q sein. Ein Vielfaches von q ist aber immer $\equiv 0 \; mod \; q$, stellt also dieselbe Wurzel wie $x = 0$ dar.

X. Wenn der Model q in D enthalten ist, aber ein vollkommenes Quadrat a^2 darstellt; so hat die Kongruenz (1) a Wurzeln, nämlich $x = 0$, a, $2a$, $\ldots (a-1)a$.

Dieser Satz leuchtet ein, wenn man erwägt, dass jetzt x nothwendig ein Vielfaches von a sein muss.

XI. Der vorstehende Satz erleichtert die Auflösung der Kongruenz $D \equiv x^2 \; mod \; q$ für den Fall, dass D und q irgend ein Quadrat zum gemeinschaftlichen Faktor haben, dass also $D = a^2 D'$, $q = a^2 q'$ ist. Man braucht in diesem Falle offenbar nur die Kongruenz $D' \equiv x'^2 \; mod \; q'$ zu lösen. Jeder hierdurch gefundene Werth von x' liefert sofort a Wurzeln der ersteren Kongruenz in der Form $x = ax'$, $a(x' + q')$, $a(x' + 2q') \ldots a[x' + (a-1)q']$ und man erkennt, dass die erstere Kongruenz a mal so viel Wurzeln besitzt, als die letztere.

XII. Wenn endlich der Model q irgend eine zusammengesetzte Zahl ist, welche mit D irgend ein gemeinschaftliches Maass besitzt; so bestimmt man die Anzahl der Wurzeln der Kongruenz (1) mit Hülfe der vorhergehenden Sätze leicht folgendermaassen.

Kommt ein den beiden Zahlen D und q gemeinschaftlicher Primfaktor öfter in q, als in D vor; so erkennt man sofort nach §. 150, XI., dass die Kongruenz (1) unmöglich sei.

Liegt dieser Fall nicht vor, und ist überhaupt die Kongruenz (1) lösbar, was nach §. 150 oder 151 leicht ermittelt werden kann; so sei das grösste gemeinschaftliche Maass von D und q gleich a^2b, worin a^2 den grössten darin enthaltenen quadratischen Faktor, also b einen nur aus ersten Potenzen verschiedener Primzahlen bestehenden Faktor darstellt. Nach Absonderung dieses grössten gemeinschaftlichen Maasses aus dem Werthe des Models q, bleibe der Faktor $2^v r^m s^n \ldots$ zurück, worin $r, s \ldots$ im Ganzen w verschiedene unpaare Primzahlen darstellen, von denen auch keine in dem nichtquadratischen Faktor b enthalten sein wird, wol aber in dem quadratischen Faktor a^2 vorkommen kann. Man habe also

(9) $D = a^2D'$ $\quad q = a^2q'$

(10) $D' = bD''$ $\quad q' = b2^v r^m s^n \ldots$

Wegen des quadratischen Faktors a^2 können die Wurzeln der Kongruenz $D \equiv x^2 \bmod q$ nach dem obigen Satze XI. leicht aus denen der Kongruenz $D' \equiv x'^2 \bmod q'$ abgeleitet werden, und man weiss, dass Dies für die erstere Kongruenz a mal so viel Wurzeln, als für die letztere ergeben wird.

Was nun die Anzahl der Wurzeln der letzteren Kongruenz betrifft; so ist nach den obigen Sätzen die Anzahl der Wurzeln der Kongruenz

$D' \equiv x'^2 \bmod b$ gleich 1

$D' \equiv x'^2 \bmod 2^v$ » $u = 1, 2, 4$, jenachdem $v = 1, 2, > 2$ ist.

$D' \equiv x'^2 \bmod r^m$ » 2

$D' \equiv x'^2 \bmod s^n$ » 2

u. s. w. Da nun von den Faktoren $b, 2^v, r^m, s^n \ldots$ je zwei relativ prim sind; so bilden sich die Wurzeln der Kongruenz $D' \equiv x'^2 \bmod q'$ durch Kombination der Wurzeln der vorstehenden Kongruenzen. Dies gibt $u2^w$ Wurzeln für die letztere Kongruenz, also $au2^w$ Wurzeln für die gegebene Kongruenz $D \equiv x^2 \bmod q$. Wenn der Faktor 2^v ganz fehlt, hat man in der letzteren Formel auch den Faktor u wegzulassen. Man erkennt auch, dass die Anzahl der Wurzeln von dem nichtquadratischen Faktor b des gemeinschaftlichen Maasses der beiden Zahen D und q ganz unabhängig ist.

XIII. Beispiele. Nach §. 150, XIV. ist die Kongruenz (1) für $D = 2^2 . 5^2 . 13$ und $q = 2^4 . 5^2 . 13$ lösbar. Hier hat man $D = (2 . 5)^2 . 13$, $q = (2 . 5)^2 . 13 . 2^2$ also $a = 2 . 5 = 10$, $b = 13$, $v = 2$, $w = 0$, $u = 2$. Die Anzahl der Wurzeln ist also $10 . 2 = 20$.

Wäre $D = 5 . 3^2 . 7$, $q = 5 . 19 . 23$ gegeben; so ist die Kongruenz (1) möglich, und man hat $a = 1$, $b = 5$, $w = 2$. Die Anzahl der Wurzeln ist also $= 2^2 = 4$.

Wäre $D = 7 . 13$, $q = 2 . 3^2 . 5$ gegeben; so ist die Kongruenz (1) möglich, und man hat $a = 1$, $b = 1$, $v = 1$, $w = 2$, $u = 1$, also $2^2 = 4$ Wurzeln.

Wäre $D = 3^4 . 19$, $q = 3^2$ gegeben; so ist die Kongruenz (1) möglich, und man hat $a = 3$, $w = 0$, also 3 Wurzeln.

Wäre $D = 3^4 . 19$, $q = 3^3$; so hat man $a = 3$, $b = 3$, $w = 0$, also ebenfalls 3 Wurzeln.

XIV. Wenn in der gegebenen quadratischen Kongruenz das Quadrat der Unbekannten noch mit einem Faktor behaftet ist, wenn also die Kongruenz

(11) $$ax^2 \equiv b \mod q$$

gegeben ist; so bewirkt man deren Auflösung, indem man erst die Kongruenz ersten Grades

(12) $$ay \equiv b \mod q$$

und alsdann für den hieraus sich ergebenden einzigen Werth von y, welcher $< q$ ist, die quadratische Kongruenz

(13) $$x^2 \equiv y \mod q$$

auflös't, welche Letztere für x mehrere Werthe $< q$ ergeben kann.

Man kann auch, nachdem man die gegebene Kongruenz mit a multiplizirt hat, wodurch dieselbe

(14) $$(ax)^2 \equiv ab \mod q$$

wird, erst die quadratische Kongruenz

(15) $$y^2 \equiv ab \mod q$$

und alsdann für jeden hieraus sich ergebenden Werth von y, welcher positiv und $< q$ oder welcher positiv oder negativ und numerisch $\leqq \frac{q}{2}$ ist, die Kongruenz ersten Grades

(16) $$ax \equiv y \mod q$$

auflösen, welche für x eben so viel Werthe $< q$ ergibt, als für y gefunden waren.

XV. Was endlich die allgemeinste Form der quadratischen Kongruenz

(17) $$ax^2 - 2bx - c \equiv 0 \mod q$$

anlangt; so kann man immer voraussetzen, nöthigenfalls durch Multiplikation mit 2 bewirken, dass der Koeffizient des in x multiplizirten Gliedes eine paare Zahl ist.

Multiplizirt man die Kongruenz (17) mit a und setzt $b^2 + ac = D$; so kommt

(18) $$(ax - b)^2 \equiv D \mod q$$

Demnach lös't man erst die quadratische Kongruenz

(19) $$y^2 \equiv D \mod q$$

und hierauf für jeden sich ergebenden Werth von y, welcher

positiv und $< q$ oder welcher positiv oder negativ und absolut $\leqq \frac{q}{2}$ ist, die Kongruenz ersten Grades

$$ax - b \equiv y \mod q \quad \text{oder}$$
(20) $$ax \equiv b + y \mod q$$

Will man die Auflösung der Kongruenz (17) durch unmittelbare Substitution sukzessiver Werthe für x bewirken; so ist es nicht nöthig, dass der Koeffizient von x eine paare Zahl sei. Man verfährt dann einfach in folgender Weise. Indem man die gegebene Kongruenz (17) in die Form

(21) $$ax^2 + bx \equiv c \mod q$$

stellt, nimmt man für die drei konstanten Zahlen a, b, c ihre kleinsten positiven Reste nach q. Beachtet man jetzt, dass wenn x um 1 wächst, die linke Seite der Kongruenz (21) um $2ax + a + b = (2x + 1)a + b$ wächst; so ist klar, dass man, wenn man mit dem Werthe $x = 0$ beginnt, wodurch die linke Seite jener Kongruenz selbst $= 0$ wird, zu den sukzessiv sich ergebenden Werthen für jene linke Seite nach und nach nur die Zahlen $a + b$, $3a + b$, $5a + b$, $7a + b$ u. s. w. oder deren kleinste positiven Reste nach q hinzuzuaddiren braucht, indem man vor jeder neuen Addition immer erst die ganze linke Seite der Kongruenz (21) auf ihren kleinsten positiven Rest reduzirt. Diese Rechnung ist bis zu dem Werthe $x = q - 1$ fortzusetzen. So oft hierbei der Rest der linken Seite der Kongruenz (21) gleich c wird, hat man in dem zugehörigen Werthe von x eine Auflösung gefunden, welcher immer eine unendliche Reihe kongruenter Wurzeln in der Form $x + vq$ entspricht.

Wäre z. B. die Kongruenz

$$24x^2 - 51x \equiv 43 \mod 7$$

gegeben; so hat man zunächst durch Reduktion der Koeffizienten 24, -51, 43 auf ihre kleinsten positiven Reste

$$3x^2 + 5x \equiv 1 \mod 7$$

Die sukzessiv zu addirenden Zahlen $a + b$, $3a + b$ u. s. w. sind jetzt 8, 14, 20, 26, 32, 38 oder deren kleinste positiven Reste 1, 0, 6, 5, 4, 3. Man erhält also folgende Rechnung

x	Reste von $(2x + 1)a + b$	Reste von $3x^2 + 5x$
0	1	0
1	0	1
2	6	1
3	5	0
4	4	5
5	3	2
6		5

Unter den Resten von $3x^2 + 5x$ sind nur zwei $\equiv 1$, und dieselben entsprechen den beiden Wurzeln $x = 1$, $x = 2$.

§. 153. ***Lineare Form der Primfaktoren von $D - x^2$.***

I. Nach Gauss, *Disq. arithm. art.* 147, 148, 149, lässt sich der Fundamentalsatz, §. 149, in Verbindung mit dem Satze §. 151, dazu verwenden, um eine sehr interessante einfache lineare Form, d. h. eine Form ersten Grades nachzuweisen, welcher die Primfaktoren der Zahlform $\pm D - x^2$ entsprechen.

Wir suchen also die Form der Primzahlen q, welche die Gleichung $\pm D - x^2 = vq$ oder die Kongruenz $\pm D \equiv x^2 \, mod \, q$ erfüllen, d. i. derjenigen, nach welchen die Determinante $\pm D$ ein quadratischer Rest ist oder für welche man $\pm DRq$ hat, wobei wir die in D selbst enthaltenen Primzahlen, welche auch stets Faktoren von $\pm D - x^2$ sind, unbeachtet lassen.

Zu diesem Ende können wir offenbar voraussetzen, dass die Primzahl q positiv sei. Was die Determinante $\pm D$ betrifft, welche sowol positiv wie negativ sein kann; so wollen wir unter D stets eine positive Zahl verstehen.

Es hat keine Schwierigkeit, von allen positiven Zahlen, welche unterhalb einer gegebenen Gränze liegen und relativ prim zu D sind, diejenigen zu ermitteln, welche quadratische Reste nach D sind. Das allgemeine Zeichen für irgend Einen dieser Reste sei r, sodass man $r \equiv x^2 \, mod \, D$ oder rRD hat. Es leuchtet ein, dass jeder Rest r eine besondere Reihe von quadratischen Resten nach D liefert, deren allgemeines Glied durch $wD + r$ dargestellt ist, wenn man mit w jede beliebige ganze Zahl bezeichnet, sodass man also allgemein

(1) $$(wD + r)RD$$

hat. Diejenigen unterhalb derselben Gränze liegenden und zu D relativ primen Zahlen, welche unter den quadratischen Resten r nicht vorkommen, sind quadratische Nichtreste nach D, und wenn man irgend Einen derselben mit s bezeichnet, hat man allgemein

(2) $$(wD + s)ND$$

Da wir auf die Darstellung von Primzahlen ausgehen; so ist klar, warum die Reste r und Nichtreste s nur unter den zu D relativ primen Zahlen ausgesucht werden, indem, wenn z. B. r und D ein gemeinschaftliches Maass hätten, auch $wD + r$ und D ein solches besässen, also $q = wD + r$ keine Primzahl sein könnte. Hierdurch ist nur diejenige begränzte Menge von Primzahlen ausgeschlossen, welche in D selbst, also auch stets in $D - x^2$ enthalten sind.

Wir spezialisiren nunmehr das Problem etwas abweichend von der Darstellung der *Disq. arithm.* folgendermaassen, indem

wir vorweg bemerken, dass in allen Fällen $q=1$ und auch $=2$ sein kann, weshalb diese beiden Werthe von q nicht weiter berücksichtigt werden.

II. Es sei die positive Determinante $D=1$. Alsdann kann nach §. 149, V. die Primzahl q jeden beliebigen Werth annehmen, indem man immer $1Rq$ hat. Die Form $1-x^2$ enthält also jede Primzahl als Faktor.

III. Es sei die negative Determinante $-D=-1$. Alsdann ist jede Primzahl q von der Form $4n+1$ ein Faktor, aber jede Primzahl von der Form $4n+3$ kein Faktor von $-1-x^2$ oder von $1+x^2$. Denn nach §. 149, VIII. hat man, wenn $q=4n+1$ ist,

(3) $$1Rq \quad \text{und} \quad -1Rq$$

wenn jedoch $q=4n+3$ ist,

(4) $$1Rq \quad \text{und} \quad -1Nq$$

IV. Es sei die positive Determinante $D=2$. Alsdann sind alle Primzahlen q von der Form $8n+1$ und $8n+7$ Faktoren, dagegen alle Primzahlen von der Form $8n+3$ und $8n+5$ keine Faktoren von $2-x^2$. Dies erhellet sofort aus §. 149, VI.

V. Es sei die negative Determinante $-D=-2$. Alsdann sind alle Primzahlen q von der Form $8n+1$ und $8n+3$ Faktoren, dagegen alle Primzahlen von der Form $8n+5$ und $8n+7$ keine Faktoren von $-2-x^2$ oder von $2+x^2$, was aus §. 149, VII. hervorgeht.

VI. Es sei die Determinante D eine positive Primzahl von der Form $4m+1$. Ist dann r irgend ein quadratischer Rest nach D, kleiner als D, und s irgend ein quadratischer Nichtrest nach D, kleiner als D; so sind alle Primzahlen q von der Form $wD+r$ Faktoren, dagegen alle Primzahlen von der Form $wD+s$ keine Faktoren von $D-x^2$.

Denn nach dem Fundamentalsatze §. 149 folgt nun aus

(5) $$(wD+r)RD \quad \text{und} \quad (wD+s)ND$$

sofort

(6) $$DR(wD+r) \quad \text{und} \quad DN(wD+s)$$

Wäre z. B. $D=13$; so sind die quadratischen Reste $r=1, 3, 4, 9, 10, 12$ und die quadratischen Nichtreste $s=2, 5, 6, 7, 8, 11$. Demnach sind alle Primzahlen, welche Einer der Formen $13w+1$, $13w+3$, $13w+4$, $13w+9$, $13w+10$, $13w+12$ entsprechen, Faktoren, diejenigen Primzahlen jedoch, welche Einer der Formen $13w+2$, $13w+5$, $13w+6$, $13w+7$, $13w+8$, $13w+11$ entsprechen, keine Faktoren von $13-x^2$.

VII. Es sei die Determinante $-D$ eine negative Primzahl von der Form $-(4m+1)$. Haben dann r und s die vorstehende Bedeutung von Resten und Nichtresten; so sind alle Primzahlen, welche gleichzeitig der Form $wD+r$ und $4n+1$, sowie diejenigen, welche gleichzeitig der Form $wD+s$ und $4n+3$ entsprechen, Faktoren, dagegen alle Primzahlen, welche gleichzeitig der Form $wD+r$ und $4n+3$, sowie diejenigen, welche gleichzeitig der Form $wD+s$ und $4n+1$ entsprechen, keine Faktoren von $-D-x^2$ oder von $D+x^2$.

Denn nach dem Fundamentalsatze §. 149 erhält man wie sub VI. aus den Beziehungen (5) zunächst die Beziehungen (6). Aus (6) folgt aber nach §. 149, IV., wenn die Primzahl $wD+r$ oder $wD+s$ die Form $4n+1$ hat,

(7) $\qquad -DR(wD+r) \qquad -DN(wD+s)$

und wenn diese Primzahl die Form $4n+3$ hat,

(8) $\qquad -DN(wD+r) \qquad -DR(wD+s)$

Die im Vorstehenden enthaltene Trennung der gesuchten Primzahlen nach den beiden Formklassen $4n+1$ und $4n+3$ kann nach der weiter unten folgenden Bemerkung sub XIII. leicht beseitigt werden.

VIII. Es sei die Determinante D eine positive Primzahl von der Form $4m+3$. Haben dann r und s die vorstehende Bedeutung; so sind alle Primzahlen, welche gleichzeitig der Form $wD+r$ und $4n+1$, sowie diejenigen, welche gleichzeitig der Form $wD+s$ und $4n+3$ entsprechen, Faktoren, dagegen alle Primzahlen, welche gleichzeitig der Form $wD+r$ und $4n+3$, sowie diejenigen, welche gleichzeitig der Form $wD+s$ und $4n+1$ entsprechen, keine Faktoren von $D-x^2$.

Denn jetzt folgt nach dem Fundamentalsatze aus den Beziehungen (5) nur dann die betreffende der Beziehungen (6), wenn die links neben R oder N stehende Primzahl die Form $4n+1$ besitzt. Sobald dieselbe die Form $4n+3$ besitzt, hat man in der betreffenden der Beziehungen (6) wegen §. 149, IV. links vor D das negative Zeichen zu setzen. Hierauf ergibt sich der vorstehende Satz sehr leicht.

Auch hier kann die Trennung der gesuchten Primzahlen in die beiden Formklassen $4n+1$ und $4n+3$ nach XIII. leicht beseitigt werden.

Wäre z. B. $D=3$; so ist $r=1$, $s=2$. Es sind also die Primzahlen von den gemeinschaftlichen Formen $3w+1$, $4n+1$ oder $3w+2$, $4n+3$ Faktoren, dagegen die von den gemeinschaftlichen Formen $3w+1$, $4n+3$ oder $3w+2$, $4n+1$ keine Faktoren von $3-x^2$.

IX. Es sei die Determinante $-D$ eine negative Primzahl von der Form $-(4m+3)$. Haben dann r und s die vor-

stehende Bedeutung; so sind alle Primzahlen von der Form $wD+r$ Faktoren, dagegen alle Primzahlen von der Form $wD+s$ keine Faktoren von $-D-x^2$ oder von $D+x^2$.

Auch dieser Satz ergibt sich leicht nach den Andeutungen sub VIII.

Wäre z. B. $-D=-11$; so sind die Reste $r=1, 3, 4, 5, 9$ und die Nichtreste $s=2, 6, 7, 8, 10$. Folglich sind die Primzahlen von Einer der Formen $11w+1, 3, 4, 5, 9$ Faktoren, dagegen die Primzahlen von Einer der Formen $11w+2, 6, 7, 8, 10$ keine Faktoren von $11+x^2$.

Wäre $-D=-3$; so ist $r=1$, $s=2$; also sind die Primzahlen von der Form $3w+1$ Faktoren, dagegen die von der Form $3w+2$ keine Faktoren von $3+x^2$.

X. Was die Fälle betrifft, wo die Determinante eine zusammengesetzte Zahl ist; so sind zunächst alle Faktoren von D auch Faktoren von $\pm D-x^2$. Diese Faktoren wollen wir, wie schon oben bemerkt, bei der ferneren Untersuchung ausser Acht lassen, also nur solche Primzahlen q betrachten, welche in D nicht enthalten sind.

Hätte nun D einen quadratischen Faktor α^2, sodass $D=\alpha^2D'$ wäre; so könnte man denselben unterdrücken, und D' für D nehmen. Denn alle (nicht in D aufgehenden) Primzahlen q, welche Faktoren oder keine Faktoren von $D'-x^2$ sind, stehen auch in derselben Beziehung zu $\alpha^2D'-x^2$. Weil nämlich stets $(\alpha^2)^{\frac{q-1}{2}}=\alpha^{q-1}\equiv 1 \mod q$ oder $\alpha^2 Rq$ ist; so hat man, wenn $D'Rq$ oder $D'^{\frac{q-1}{2}}\equiv 1 \mod q$ ist, $(\alpha^2D')^{\frac{q-1}{2}}\equiv 1 \mod q$, folglich auch $(\alpha^2D')Rq$, und wenn $D'Nq$ ist, auch $(\alpha^2D')Nq$. Hierin kann man auch $-D'$ statt D' setzen.

Nunmehr kann man folgende drei Fälle unterscheiden:

erstens, wenn die Determinante positiv und von der Form $4m+1$ oder negativ und von der Form $-(4m+3)$ ist,

zweitens, wenn dieselbe positiv und von der Form $4m+3$ oder negativ und von der Form $-(4m+1)$ ist,

drittens, wenn dieselbe positiv oder negativ paar, also von Einer der Formen $\pm 2(4m+1)$, $\pm 2(4m+3)$ ist.

XI. Wenn die Determinante dem ersten Falle angehört; so sei der absolute Werth D in seine Primfaktoren zerlegt. Von diesen Primfaktoren habe ein Theil, nämlich $a, b, c\ldots$ die Form $4n+1$ und der andere Theil, nämlich $\alpha, \beta, \gamma\ldots$ die Form $4n+3$. Jenachdem $D=4m+1$ oder $=4m+3$ ist, wird die Anzahl der letzteren Faktoren resp. paar oder unpaar sein, sodass in beiden Fällen die Determinante nicht bloss nach ihrem absoluten Werthe, sondern auch nach ihrem

Zeichen dargestellt wird, wenn man die letzteren Faktoren α, β, γ... negativ nimmt. Schreiben wir also

(9) $$D = a.b.c\ldots\alpha.\beta.\gamma\ldots$$

so ist, wenn wir den vollständigen Werth der Determinante mit D' bezeichnen,

(10) $$D' = \pm D = a.b.c\ldots(-\alpha)(-\beta)(-\gamma)\ldots$$

Theilt man nun alle Zahlen, welche kleiner als D und relativ prim zu D sind, in zwei Klassen, stellt in die erste Klasse alle diejenigen, welche quadratische Nichtreste nach keiner, nach zwei, nach vier und überhaupt nach einer paaren Menge der Faktoren a, $b\ldots\alpha$, $\beta\ldots$, sind, dagegen in die zweite Klasse alle diejenigen, welche quadratische Nichtreste nach Einer, nach drei, nach fünf und überhaupt nach einer unpaaren Menge jener Faktoren sind, bezeichnet die Zahlen in der ersten Klasse mit r und die in der zweiten mit s; so sind alle Primzahlen von der Form $wD + r$ Faktoren, dagegen alle Primzahlen von der Form $wD + s$ keine Faktoren von $D' - x^2$.

Um Dies einzusehen; so sei q eine Primzahl von der Form $wD + r$ und zwar quadratischer Nichtrest nach keinem der Faktoren a, $b\ldots\alpha$, $\beta\ldots$, also quadratischer Rest nach jedem dieser Faktoren. Alsdann hat man nach der Voraussetzung

(11) $$qRa \qquad qRb \qquad \ldots \qquad qR\alpha \qquad qR\beta \qquad \ldots$$

Hieraus folgt nach dem Fundamentalsatze und nach §. 149, V., welche Form auch q haben möge,

(12) $$aRq \qquad bRq \qquad \ldots \qquad -\alpha Rq \qquad -\beta Rq \qquad \ldots$$

Hieraus folgt, da $ab\ldots(-\alpha)(-\beta)\ldots = D'$ ist, $D'Rq$.

Lässt man nun q quadratischen Nichtrest nach einer paaren Menge der Faktoren a, $b\ldots\alpha$, $\beta\ldots$ sein; so verwandelt sich eine paare Menge der Zeichen R in den Formeln (11), sowie in den Formeln (12) in das Zeichen N. Dies hat aber nach §. 151 immer den Schluss $D'Rq$ zur Folge.

Lässt man dagegen q quadratischen Nichtrest nach einer unpaaren Menge der fraglichen Faktoren sein; so verwandelt sich in eben gedachter Weise eine unpaare Menge der Zeichen R in N, und Dies hat nach §. 151 den Schluss $D'Nq$ zur Folge.

Aus den *Disq. arithm. art.* 148 entlehnen wir folgendes Beispiel. Wenn $D = 105 = 3.5.7$ ist; so hat man

$r =$ 1, 4, 16, 46, 64, 79 als Nichtreste nach keinem der Faktoren 3, 5, 7
$=$ 2, 8, 23, 32, 53, 92 als Nichtreste nach den beiden Faktoren 3, 5
$=$ 26, 41, 59, 89, 101, 104 als Nichtreste nach den beiden Faktoren 3, 7
$=$ 13, 52, 73, 82, 97, 103 als Nichtreste nach den beiden Faktoren 5, 7

ferner

$s =$ 11, 29, 44, 71, 74, 86 als Nichtreste nach dem Faktor 3
$=$ 22, 37, 43, 58, 67, 88 als Nichtreste nach dem Faktor 5
$=$ 19, 31, 34, 61, 76, 94 als Nichtreste nach dem Faktor 7
$=$ 17, 38, 47, 62, 68, 83 als Nichtreste nach den drei Faktoren 3, 5, 7

XII. Wenn die Determinante dem zweiten oder dem dritten Falle angehört; so kann dieselbe, wenn wir sie mit D'' bezeichnen, stets in die Form

$$(13) \qquad D'' = kD'$$

gebracht werden, worin D' eine Zahl von der Form der sub XI. betrachteten und nach Gl. (10) zerlegten Determinante darstellt, während der Koeffizient k entweder -1 oder 2 oder -2 ist.

Aus §. 151 leuchtet ein, dass D'' ein quadratischer Rest nach allen denjenigen Primzahlen q ist, nach welchen die beiden Zahlen D' und k zu gleicher Zeit quadratische Reste oder Nichtreste sind, dass dagegen D'' ein quadratischer Nichtrest nach allen denjenigen Primzahlen q ist, nach welchen die Eine der beiden Zahlen D' und k quadratischer Rest und die andere Nichtrest ist. In Zeichen:

wenn	$D'Rq$	$D'Nq$	$D'Rq$	$D'Nq$
und	kRq	kNq.	kNq	kRq
so ist	$D''Rq$	$D''Rq$	$D''Nq$	$D''Nq$

Besitzen nun r und s genau die Bedeutung aus XI., wobei D der absolute Werth von D' nach Gl. (9) ist; so ergibt sich resp. für $k = -1, 2, -2$ aus einer Zusammenstellung der Resultate resp. aus XI. und III., aus XI. und IV., aus XI. und V. für die Form der Primzahlen q, welche Faktoren und welche keine Faktoren von $D'' - x^2$ sind, die folgende Tabelle, welche so zu verstehen ist, dass die betreffende Primzahl der zu oberst notirten Form $wD + r$ oder $wD + s$ und gleichzeitig irgend Einer der darunter stehenden, neben dem zugehörigen Werthe von k notirten Form entsprechen muss.

k	Faktoren		keine Faktoren	
	$wD + r$	$wD + s$	$wD + r$	$wD + s$
-1	$4n + 1$	$4n + 3$	$4n + 3$	$4n + 1$
2	$8n + 1$ $8n + 7$	$8n + 3$ $8n + 5$	$8n + 3$ $8n + 5$	$8n + 1$ $8n + 7$
-2	$8n + 1$ $8n + 3$	$8n + 5$ $8n + 7$	$8n + 5$ $8n + 7$	$8n + 1$ $8n + 3$

Es leuchtet ein, dass in jedem Falle jede Primzahl in irgend Eine der vorstehend bezeichneten Kategorieen fallen muss, also stets als **Faktor** oder als **kein Faktor** erkannt werden kann.

XIII. In den zuletzt sub XII., sowie in den sub VII. und VIII. erörterten Fällen, erscheinen sowol die Primzahlen, welche Faktoren, als auch diejenigen, welche keine Faktoren sind, nach mehreren allgemeinen Formklassen wie $4n+1$, $4n+3$, $8n+1$, $8n+3$ etc. getrennt. Diese Trennung kann folgendermaassen leicht beseitigt werden.

In den Fällen, wo die gedachte Trennung nach Klassen von der Form $4n+1$ und $4n+3$ erforderlich ist, hebe man unter allen Zahlen, welche kleiner und relativ zu $4D$ sind, diejenigen, welche nach Maassgabe der obigen Formeln Faktoren sind, heraus; irgend Eine derselben sei $=t$. Ebenso ermittele man unter den bezeichneten Zahlen diejenigen, welche nach Maassgabe der obigen Formeln keine Faktoren sind; irgend Eine derselben sei $=u$.

Alsdann sind ohne Klassenunterschied alle Primzahlen von der Form $4wD+t$ Faktoren, alle übrigen von der Form $4wD+u$ keine Faktoren.

In den anderen Fällen, wo die Sonderung der Primzahlen nach Klassen von der Form $8n+1$, $8n+3$, $8n+5$, $8n+7$ erforderlich ist, ermittele man die Werthe t und u unter den Zahlen, welche $< 8D$ sind.

Die Primzahlen von der Form $8wD+t$ sind alsdann ohne Klassenunterschied Faktoren, dagegen die von der Form $8wD+u$ keine Faktoren.

Um z. B. für das sub VIII. angeführte Beispiel $D=3$ die Klassentrennung aufzuheben; so findet man nach den dortigen Formeln, dass unter den Zahlen, welche kleiner und relativ prim zu $4.3=12$ sind, $t=1$, 11 Faktoren, dagegen $u=5$, 7 keine Faktoren sind. Demnach ist jede Primzahl ohne Klassenunterschied von der Form $12w+1$ oder $12w+11$ ein Faktor, jede von der Form $12w+5$ oder $12w+7$ dagegen kein Faktor von $3-x^2$.

Wäre $D''=10$ gegeben; so hat man $D''=2.5$, also $k=2$, $D'=5$, $D=5$. Nach VI. ist $r=1$, 4 und $s=2$, 3. Nach XII. müssen aber die Faktoren $wD+r$ zugleich der Form $8n+1$ oder $8n+7$ und die Faktoren $wD+s$ zugleich der Form $8n+3$ oder $8n+5$ genügen. Hiernach gibt es unter den Zahlen, welche kleiner und relativ prim zu $8.5=40$ sind, folgende, welche Faktoren sind, $t=1$, 3, 9, 13, 27, 31, 37, 39. Die übrigen Zahlen unter dieser Gränze, welche keine Faktoren sind, genügen, wenn sie der Form $wD+r$ angehören, zugleich auch der Form $8n+3$ oder $8n+5$, und wenn sie der Form $wD+s$ angehören, zugleich auch der Form $8n+1$ oder $8n+7$. Dieselben sind $u=7$, 11, 17, 19, 21, 23, 29, 33. Hiernach sind alle Primzahlen von der Form

$40w + t = 40w + 1$, 3, 9, 13, 27, 31, 37, 39 Faktoren
$40w + u = 40w + 7$, 11, 17, 19, 21, 23, 29, 33 keine Faktoren von $10 - x^2$.

XIV. Wir bemerken noch, dass die Anzahl der Formen aller durch $wkD + t$ dargestellten Faktoren und aller durch $wkD + u$ dargestellten Nichtfaktoren zusammengenommen so gross ist, als die Anzahl der unterhalb kD liegenden zu kD relativ primen Zahlen, und dass hiervon immer die Hälfte den Ersteren und die Hälfte den Letzteren angehört.

§. 154. *Eigenschaften der Zahlen von der Form $x^2 - Dy^2$ und deren Faktoren.*

I. Das Produkt zweier Zahlen von der quadratischen Form $x^2 - Dy^2$, worin die Determinante D positiv oder negativ sein kann, ist wiederum von derselben Form. Auch kann ein solches Produkt (wenn nicht der Eine Faktor $= 1$ ist) auf mehr als Eine Weise in dieser Form dargestellt werden.

Denn man hat, wenn die beiden Zahlen mit $r^2 - Ds^2$ und $t^2 - Du^2$ bezeichnet werden,

$$(1) \quad \begin{cases} (r^2 - Ds^2)(t^2 - Du^2) = (rt + Dsu)^2 - D(ru - st)^2 \\ \qquad\qquad \text{und auch} = (rt - Dsu)^2 - D(ru + st)^2 \end{cases}$$

Aus diesem Satze folgt auch, dass das Produkt aus beliebig vielen Faktoren von der Form $x^2 - Dy^2$ wiederum dieselbe Form hat. Durch eine Form dieser Art, durch welche eine Zahl p dargestellt werden kann, lässt sich also auch jede Potenz von p darstellen: und wenn $p, q \ldots$ beliebige Zahlen sind, von denen eine jede durch jene Form darstellbar ist; so ist auch ein Produkt aus beliebigen Potenzen dieser Zahlen, wie $p^m q^n \ldots$ durch dieselbe Form darstellbar. Im Speziellen folgt hieraus für $D = -1$, dass das Produkt mehrerer Zahlen, welche die Summe zweier Quadrate $x^2 + y^2$ darstellen, wiederum die Summe zweier Quadrate ist.

II. Jede Primzahl q, welche sich in der Form $x^2 - Dy^2$ darstellen lässt, kann, wenn die Determinante D negativ $= -D'$, jene Form also auch $= x^2 + D'y^2$ ist, nur auf eine einzige Art in dieser Form dargestellt werden, d. h. es gibt für x und y nur ein einziges Paar zulässiger numerischer Werthe, welche man nur für den Fall, dass $D' = 1$ ist, mit einander verwechseln, deren Zeichen man jedoch stets beliebig annehmen kann.

Denn angenommen, es wäre

$$(2) \qquad r^2 + D's^2 = t^2 + D'u^2 = q$$

und hierin r von t und s von u verschieden; so hätte man

$$r^2 - t^2 = D'(u^2 - s^2) \quad \text{oder} \quad (r+t)(r-t) = D'(u+s)(u-s)$$

worin weder die linke, noch die rechte Seite $=0$ sein kann. Die Faktoren der Zahlen D', $u+s$, $u-s$ auf der rechten Seite vertheilen sich in irgend einer Weise über die beiden Zahlen $r+t$, $r-t$ auf der linken Seite, sodass Ein Theil der Faktoren von D', $u+s$, $u-s$ auf $r+t$ und der andere Theil auf $r-t$ kommt. Man kann also allgemein setzen

$$(3) \qquad \begin{cases} D' = a_1 a_2 \\ u+s = v_1 v_2 \\ u-s = w_1 w_2 \\ r+t = a_1 v_1 w_1 \\ r-t = a_2 v_2 w_2 \end{cases}$$

worin mehrere der Faktoren a_1, a_2, v_1, v_2, w_1, w_2 wol $=1$, aber keiner $=0$ sein kann.

Aus den letzteren Gleichungen ergibt sich leicht

$$(4) \qquad r = \frac{1}{2}(a_1 v_1 w_1 + a_2 v_2 w_2) \qquad s = \frac{1}{2}(v_1 v_2 - w_1 w_2)$$

Hieraus folgt, wenn man die Bedingung $D' = a_1 a_2$ berücksichtigt,

$$(5) \qquad q = r^2 + D's^2 = \frac{1}{4}(a_1 v_1^2 + a_2 w_2^2)(a_1 w_1^2 + a_2 v_2^2)$$

Wäre die Primzahl $q=2$; so leuchtet ein, dass sie nur für $D'=1$ der obigen Form (2) entsprechen und sich nur auf die einzige Weise $2 = 1^2 + 1^2$ in jener Form darstellen lässt.

Wäre die Primzahl q nicht $=2$, also unpaar; so sei zuvörderst $D'=1$. Alsdann muss von r und s, sowie von t und u die Eine paar, die andere unpaar sein. Angenommen, es seien r und t paar, dagegen s und u unpaar. Alsdann ist $u+s$ und $u-s$ paar; es muss also jedenfalls Eine der beiden Zahlen v_1, v_2 und auch Eine der beiden Zahlen w_1, w_2 paar sein. Demnach kann der Ausdruck (5) für q

$$\text{entweder } q = \left[a_1\left(\frac{v_1}{2}\right)^2 + a_2\left(\frac{w_2}{2}\right)^2\right](a_1 w_1^2 + a_2 v_2^2)$$

$$\text{oder } q = (a_1 v_1^2 + a_2 w_2^2)\left[a_1\left(\frac{w_1}{2}\right)^2 + a_2\left(\frac{v_2}{2}\right)^2\right]$$

geschrieben werden, und es leuchtet ein, dass jeder der beiden Faktoren, in welche hiernach q zerfällt, >1 ist. Unter solchen Umständen kann aber q keine Primzahl sein.

Hieraus folgt, dass eine Primzahl q nur auf eine einzige Art als die Summe zweier Quadrate x^2+y^2 dargestellt werden kann, wenn sie überhaupt eine solche Darstellung zulässt.

Nehmen wir jetzt an, D' sei >1; so ist in der Gl. (5) jede der beiden Zahlen $a_1 v_1^2 + a_2 w_2^2$ und $a_1 w_1^2 + a_2 v_2^2 \geqq 3$.

Hieraus folgt, dass nach Gl. (5) die Zahl q nicht in der Form

$$q = \left(\frac{a_1 v_1^2 + a_2 w_2^2}{2}\right)\left(\frac{a_1 w_1^2 + a_2 v_2^2}{2}\right)$$

erscheinen kann, sodass jeder dieser beiden in Klammern geschlossenen Faktoren eine ganze Zahl sei, weil ein jeder dieser beiden Faktoren $\geqq \frac{3}{2}$, also > 1, mithin q keine Primzahl sein würde.

Es könnte also q nur

$$\text{entweder } q = \left(\frac{a_1 v_1^2 + a_2 w_2^2}{4}\right)(a_1 w_1^2 + a_2 v_2^2)$$

$$\text{oder } q = (a_1 v_1^2 + a_2 w_2^2)\left(\frac{a_1 w_1^2 + a_2 v_2^2}{4}\right)$$

sein. Die Eine dieser beiden Formen ist wie die andere zu behandeln. Setzen wir die erste voraus; so ist schon mehrmals bemerkt, dass der zweite Faktor in dieser Form, nämlich $a_1 w_1^2 + a_2 v_2^2 > 1$ ist. Soll also q eine Primzahl sein; so muss

$$\frac{a_1 v_1^2 + a_2 w_2^2}{4} = 1 \qquad \text{oder} \qquad a_1 v_1^2 + a_2 w_2^2 = 4$$

sein. Dieses ist aber, da von den Zahlen a_1, a_2, v_1, w_2 keine $= 0$ sein kann, nur möglich, wenn $v_1 = 1$ und $w_1 = 1$ ist, und zwar auf zweierlei Weise. Nämlich

erstens, indem $a_1 = 2$ und $a_2 = 2$ ist. Aber dann ist der zweite Faktor $a_1 w_1^2 + a_2 v_2^2$ von q eine paare Zahl, mithin q keine Primzahl;

zweitens, indem $a_1 = 1$ und $a_2 = 3$ ist. Aber dann ist nach der obigen Formel für s in (4) $s = \frac{1}{2}(v_2 - w_1)$ und da $w_1 = 1$ sein soll, v_2 ebenso wie w_1 unpaar, mithin der zweite Faktor $a_1 w_1^2 + a_2 v_2^2$ von q eine paare Zahl, folglich q keine Primzahl.

Hiernach ist der Satz bewiesen, dass wenn D' positiv ist, eine Primzahl q, welche in die Form $x^2 + D'y^2$ gebracht werden kann, nur auf eine einzige Weise so dargestellt werden kann.

Die Bedingung, dass D' positiv sei, ist wesentlich, indem für ein negatives D' (oder für eine positive Determinante D) allerdings eine Primzahl auf mehrfache Weise in der obigen Form enthalten sein kann.

III. Jede Zahl von der Form $x^2 - Dy^2$ mit relativ primen Werthen von x und y ist ein Faktor der Zahlform $x^2 - D$, und da eine Zahl von der letzteren Form in

der Gestalt $x^2 - D.1^2$ nur ein spezieller Fall der ersteren Form ist; so kann man auch sagen, dass jede Zahl von der Form $x^2 - Dy^2$ mit relativ primen Werthen von x und y der Faktor einer Zahl von derselben Form sei.

Denn ist k der Werth der ersteren Zahl; so ist nach dem fünften Abschnitte die unbestimmte Gleichung $x^2 - Dy^2 = k$ in relativ primen Zahlen nur möglich, wenn k ein Faktor von $D - x^2$ oder von $x^2 - D$ ist.

Allgemeiner erkennt man durch dieselbe Betrachtung, dass jede durch die quadratische Form $ax^2 - 2bxy - cy^2$ von der Determinante D dargestellte Zahl k ein Faktor der Zahlform $D - x^2$ ist.

IV. Alle Zahlen, welche Faktoren von Einer der beiden Zahlformen $x^2 - Dy^2$ und $x^2 - D$ sind, sind es auch von der anderen; beide Zahlformen haben also resp. die nämlichen Faktoren, wobei jedoch vorausgesetzt wird, dass in der ersteren Form x und y relativ prim seien.

Denn da nach dem vorhergehenden Satze die Zahl $x^2 - Dy^2$ ein Faktor der Zahlform $x^2 - D$ ist; so ist jeder ihrer Faktoren auch ein Faktor der Zahlform $x^2 - D$. Und umgekehrt, da die Zahl $x^2 - D = x^2 - D.1^2$ nur ein spezieller Fall der allgemeineren Form $x^2 - Dy^2$ ist; so ist jeder ihrer Faktoren auch ein Faktor der letzteren Form.

V. Je zwei Faktoren q, r, in welche sich eine Zahl von der Form $x^2 - Dy^2$ mit relativ primen Werthen von x und y zerlegen lässt, können durch zwei quadratische Formen von folgender Beschaffenheit dargestellt werden.

(6) $$q = qx^2 - 2pxy - rsy^2$$

(7) $$r = rx^2 - 2psy - qsy^2$$

In jeder dieser Formen ist die Determinante $p^2 + qrs = D$ und x, y sind relativ prim (ohne jedoch in beiden Formen dieselben Werthe zu besitzen).

Denn nach dem obigen Satze III. ist die gegebene Zahl $x^2 - Dy^2$ ein Faktor einer Zahl von der Form $D - x^2$. Für einen gewissen Werth von p hat man also $D - p^2 = qrs$ oder $D = p^2 + qrs$. Hieraus und aus dem fünften Abschnitte leuchtet sofort ein, dass sowol die unbestimmte Gl. (6), als auch die Gl. (7) in ganzen und relativ primen Zahlen lösbar ist, indem man z. B. für die erste $K = \frac{\sqrt{D} + p}{q}$ hat und $K' = \frac{\sqrt{D} + p}{q}$ nehmen kann, was sofort zu zulässigen Kombinationen zwischen K und K' führt.

Wegen der in (6) und (7) enthaltenen Form nennt man wol die Faktoren der Zahlform $x^2 - Dy^2$ schlechthin **quadratische Faktoren oder Divisoren** derselben, besser aber **Faktoren oder Divisoren von quadratischer Form.**

Je zwei Faktoren q, r, in welche sich eine Zahl von der Form $D - x^2$ zerlegen lässt, können durch zwei quadratische Formen mit der Determinante D und entgegengesetzten Koeffizienten, also folgendermaassen dargestellt werden.

(8) $$q = ax^2 - 2bxy - cy^2$$
(9) $$r = -ax^2 + 2bxy + cy^2$$

In jeder dieser Formen sind x und y relativ prim (ohne jedoch in beiden dieselben Werthe zu besitzen).

Nimmt man Einen der beiden Faktoren q oder r mit entgegengesetztem Zeichen; so wird seine Form der des andern Faktors gleich, während das Produkt aus beiden die Form $x^2 - D$ annimmt. Demnach kann man auch behaupten, dass **je zwei Faktoren, in welche sich eine Zahl von der Form $x^2 - D$ zerlegen lässt, stets durch Ein und dieselbe quadratische Form mit der Determinante D dargestellt werden können.**

Der gegenwärtige Fall entspringt, da jetzt für einen gewissen Werth von p offenbar $D - p^2 = qr$ sein muss, aus dem vorhergehenden, sobald man dort $s = 1$ annimmt. Hierdurch werden die beiden Gleichungen (6), (7)

(10) $$q = qx^2 - 2pxy - ry^2$$
(11) $$r = rx^2 - 2pxy - qy^2$$

für deren letzte man auch nach §. 124 die ihr **äquivalente**

(12) $$r = -qx^2 + 2pxy + ry^2$$

setzen kann, deren Koeffizienten die entgegengesetzten Zeichen der Koeffizienten der Form (10) besitzen, was zu beweisen war.

Es leuchtet ein, dass die beiden zusammengehörigen Faktoren q, r in allen den Fällen durch ein und dieselbe quadratische Form dargestellt werden können, wenn die Formen (10) und (11) **äquivalent** sind. Das Letztere wird sich unbedingt dann ereignen, wenn die Periode von $\frac{\sqrt{D} + p}{q}$ eine **unpaare** Gliederzahl besitzt.

Ferner ist klar, dass wenn irgend eine Form (8) bekannt ist, wodurch der Eine Faktor q dargestellt werden kann, durch Umkehrung der Zeichen der Koeffizienten sofort eine Form erhalten wird, durch welche sich der andere Faktor r darstellen lässt.

VII. Wenn man alle reduzirten Formen für die Determinante D bildet (§. 124); so erhält man sämmtliche quadratische Formen in einfachster Gestalt, welchen die Faktoren der Zahlform $x^2 - Dy^2$ oder der Zahlform $x^2 - D$ entsprechen müssen.

Zwei zusammengehörige Faktoren der Zahlform $D - x^2$ werden erhalten, wenn man irgend Eine dieser reduzirten Formen Einmal mit ihren wirklichen und Einmal mit entgegengesetzten Koeffizienten nimmt. Erzeugt Dies zwei äquivalente Formen, was man leicht prüfen kann; so stellt die betreffende reduzirte Form gleichzeitig die beiden zusammengehörigen Faktoren von $D - x^2$ dar.

Zwei zusammengehörige Faktoren der Zahlform $x^2 - D$ werden übrigens immer durch Ein und dieselbe reduzirte Form dargestellt.

Wendet man diese Betrachtungen auf die in §. 124 mitgetheilten reduzirten Formen der sukzessiv grösser werdenden positiven und negativen Determinanten an; so ergeben sich viele eigenthümliche Sätze, wovon wir hier nur einige hervorheben wollen.

Zuvörderst machen wir jedoch nochmals darauf aufmerksam, dass die nachfolgenden Sätze nur unter der ausdrücklichen Voraussetzung gelten, dass die beiden Unbekannten x, y einer Form relativ prime Zahlen seien.

VIII. Für $D = -1$ gibt es nur die einzige positive reduzirte Form $x^2 + y^2$.

Alle positiven Faktoren der Zahlform $x^2 + y^2$ oder der Zahlform $x^2 + 1$ sind also von der Form $x^2 + y^2$.

IX. Für $D = -2$ gibt es ebenfalls nur die einzige positive reduzirte Form $x^2 + 2y^2$.

Alle positiven Faktoren der Zahlform $x^2 + 2y^2$ oder der Zahlform $x^2 + 2$ sind also von der Form $x^2 + 2y^2$.

X. Für $D = -3$ gibt es die beiden positiven reduzirten Formen $x^2 + 3y^2$ und $2(x^2 + xy + y^2)$. Da x und y relativ prim sind, also nicht beide paar sein können; so stellt die erste Form $x^2 + 3y^2$ entweder nur eine unpaare Zahl oder eine paare Zahl von der Form $4n$ dar, wogegen die zweite Form nur paare Zahlen von der Form $4n + 2$ darstellen kann.

Alle positiven unpaaren und alle positiven paaren Faktoren $4n$ der Zahlform $x^2 + 3y^2$ oder der Zahlform $x^2 + 3$ sind also von der Form $x^2 + 3y^2$, wogegen alle positiven paaren Faktoren $4n + 2$ die Form $2(x^2 + xy + y^2)$ besitzen.

XI. Für $D = -4$ gibt es die beiden positiven reduzirten Formen $x^2 + 4y^2$ und $2(x^2 + y^2)$. Durch die erste werden unpaare Zahlen und paare Zahlen von der Form $4n$, durch die zweite dagegen paare Zahlen von der Form $4n$ und $4n + 2$ dargestellt.

Die positiven unpaaren Faktoren der Zahlform $x^2 + 4y^2$ oder der Zahlform $x^2 + 4$ haben also die Form $x^2 + 4y^2$, die paaren Faktoren $4n + 2$ die Form $2(x^2 + y^2)$ und die paaren Faktoren $4n$ entweder die Form $x^2 + 4y^2$ oder die Form $2(x^2 + y^2)$.

XII. Für $D = 1$ gibt es die beiden reduzirten Formen $2xy$ und $2xy + y^2$, deren letzte man offenbar auch in die Form $(x + y)^2 - x^2$, d. i. in die Form $x^2 - y^2$ bringen kann. Die erste Form stellt nur paare Zahlen, die zweite dagegen unpaare Zahlen und paare von der Form $4n$ dar.

Alle unpaaren Faktoren der Zahlform $x^2 - y^2$ oder der Zahlform $x^2 - 1$ sind also von der Form $x^2 - y^2$, welche äquivalent $2xy + y^2$ ist, alle paaren Faktoren dagegen entweder von der Form $2xy$ oder von der Form $x^2 - y^2$.

XIII. Für $D = 2$ gibt es nur die einzige reduzirte Form $x^2 - 2y^2$.

Alle Faktoren der Zahlform $x^2 - 2y^2$ oder der Zahlform $x^2 - 2$ sind also von der Form $x^2 - 2y^2$.

XIV. Für $D = 3$ gibt es die beiden reduzirten Formen $x^2 - 3y^2$ und $3x^2 - y^2$, für welche letztere man auch die Form $-(x^2 - 3y^2)$ nehmen kann.

Alle Faktoren der Zahlform $x^2 - 3y^2$ oder der Zahlform $x^2 - 3$ haben also entweder die Form $x^2 - 3y^2$ oder die Form $3x^2 - y^2$. Statt dessen kann man auch sagen, von jedem Faktor jener Zahlform habe entweder der positive oder der negative Werth die Form $x^2 - 3y^2$.

XV. Für $D = 4$ gibt es vier reduzirte Formen $4xy$, $4xy + y^2$, $4xy + 2y^2$, $4xy + 3y^2$, für welche man auch die vier Formen $4xy$, $x^2 - 4y^2$, $2(x^2 - y^2)$, $4x^2 - y^2$ nehmen kann.

Demnach sind alle unpaaren Faktoren der Zahlform $x^2 - 4y^2$ oder der Zahlform $x^2 - 4$ entweder von der Form $x^2 - 4y^2$ oder von der Form $4x^2 - y^2$. Die paaren Faktoren können jedoch von irgend Einer der bezeichneten vier Formen sein.

§. 155. **Lineare Form der durch quadratische Formen dargestellten Primzahlen.**

I. Um die linearen Formen der Primzahlen q zu untersuchen, welche sich durch eine gegebene quadratische Form

(1) $$ax^2 - 2bxy - cy^2 = q$$

darstellen lassen, kann man voraussetzen, diese Form sei reduzirt (§. 124). Bezeichnet $D = b^2 + ac$ die Determinante dieser Form; so ist schon in §. 154, III. angemerkt, dass q ein Faktor der Zahlform $D - x^2$ sei. Da man nun nach §. 153 im Stande ist, die linearen Formen aller Primfaktoren von $D - x^2$ zu bilden; so erhält man dadurch eine Reihe von linearen Formen, unter welchen allein die durch die gegebene Form (1) darstellbaren Primzahlen q zu suchen sind.

Zugleich erkennt man aus §. 153 die linearen Formen derjenigen Primzahlen, welche durch keine quadratische Form von der Determinante D darstellbar sind.

Die Primzahlen, welche nach §. 153 Faktoren von $D - x^2$ sind, und von denen offenbar eine jede durch irgend Eine quadratische Form von der Determinante D darstellbar ist, vertheilen sich über die verschiedenen reduzirten Formen dieser Determinante dergestalt, dass jede reduzirte Form eine gewisse Klasse jener Primzahlen ausschliesslich darstellt.

Um nun die einzelnen Klassen von linearen Formen zu ermitteln, welche den einzelnen reduzirten quadratischen Formen angehören, ermittelt man in der nachstehenden Weise, welche kleinsten positiven Reste der Werth jeder einzelnen der letzteren quadratischen Formen (1) für einen gewissen Model möglicher Weise annehmen kann, wenn man darin für x und y beliebige Zahlen (welche jedoch, da es sich um die Darstellung von Primzahlen q handelt, nur relativ prim zu denken sind) substituirt. Ist A der Model, nach welchem diese Untersuchung geführt wird, und r der Vertreter irgend eines Restes, welchen die Form (1) nach jenem Model anzunehmen fähig ist; so wird die lineare Form der durch die quadratische Form darstellbaren Zahlen $vA + r$ sein.

Ist ferner B der Model, nach welchem die lineare Form $wB + s$ der Primfaktoren von $D - x^2$ in §. 153 dargestellt ist; so werden offenbar nur diejenigen Primzahlen $wB + s$, welche gleichzeitig der Form $vA + r$ entsprechen, möglicherweise durch die quadratische Form (1) darstellbar sein. Gehört nun diese lineare Form $vA + r = wB + s$ für ein bestimmtes r oder s keiner anderen reduzirten quadratischen Form, als der gegebenen (1) an; so werden alle in jener linearen Form enthaltenen Primzahlen gewiss und ausschliesslich durch diese quadratische Form dar-

gestellt. Gehört dagegen jene lineare Form mehreren reduzirten quadratischen Formen zugleich an; so kann man nur schliessen, dass die darin enthaltenen Primzahlen durch irgend Eine der letzteren quadratischen Formen dargestellt werden.

Die im Vorstehenden geforderte Vergleichung zweier linearen Formen $vA+r$ und $wB+s$ setzt voraus, dass die Model A und B gleich seien, sodass dann die Identität jener beiden Formen die Gleichheit der Reste r und s erheischt. Man kann aber jene beiden Formen, wenn deren Model A und B verschieden sein sollten, stets sehr leicht nach Ein und demselben Model C, welcher der kleinste gemeinschaftliche Dividend von A und B ist, in die Form $uC+t$ bringen. Denn ist $A=ma$, $B=mb$, $C=mab$; so erhält man für jeden Werth von r anstatt der einzigen Form $vA+r$ deren b in der Form $uC+t$, wenn man t nach und nach $=r$, $A+r$, $2A+r$, $3A+r\ldots$ $(b-1)A+r$ setzt. Ebenso erhält man für jeden Werth von s anstatt der einzigen Form $wB+s$ deren a in der Form $uC+t$, wenn man t nach und nach $=s$, $B+s$, $2B+s$, $3B+s\ldots(a-1)B+s$ setzt. Wollte man z. B. die Form $12v+7$ durch den Model $60=12.5$ darstellen; so würde man folgende 5 Formen erhalten $60v+7$, 19, 31, 43, 55.

II. Um nun die linearen Formen $vA+r$ derjenigen Zahlen q zu bestimmen, welche die quadratische Form (1) überhaupt darzustellen fähig ist, wollen wir erst einige ganz einfache Fälle betrachten. Angenommen, der Koeffizient des ersten Gliedes der Form (1) sei $=1$; so kann dieselbe, da sie eine reduzirte sein soll, nach §. 124 nur x^2-Dy^2 sein. Nimmt man jetzt die Determinante D (oder deren absoluten Werth) zum Model der linearen Form an, setzt also $q=vD+r$; so hat man

(2) $$x^2-Dy^2=vD+r$$

also

(3) $$x^2\equiv r \bmod D$$

Bildet man hiernach die Reste der Quadrate der sukzessiv aufsteigenden Zahlen 0, 1, 2, 3..., also die Reste von 0, 1, 4, 9..., welche bekanntlich eine wiederkehrende Periode besitzen, und nimmt jeden derselben für r; so erhält man die linearen Formen $vD+r$, welche die durch die quadratische Form (2) darstellbaren primen oder nicht primen Zahlen nothwendig besitzen müssen. Will man nur Primzahlen betrachten; so sind für r nur diejenigen Reste zu nehmen, welche relativ prim zu D sind; der Rest 0 kann in diesem Falle immer ausser Acht bleiben.

Wäre z. B. x^2-10y^2 gegeben; so sind die Reste der Quadrate der natürlichen Zahlen nach dem Model 10 gleich 0, 1,

4, 5, 6, 9. **Durch die quadratische Form $x^2 - 10y^2$ können also nur Zahlen von der linearen Form $10v + 0, 1, 4, 5, 6, 9$** dargestellt werden. **Fragt man jedoch nach den darstellbaren** Primzahlen; so sind nur die zu 10 relativ primen Reste 1 und 9 beizubehalten. Die gesuchten Primzahlen können also nur die lineare Form $10v + 1$ oder $10v + 9$ haben.

III. Hat der absolute Werth des ersten Koeffizienten der gegebenen quadratischen Form den absoluten Werth der Determinante; so kann jene Form nur $Dx^2 \pm y^2$ sein. Nimmt man jetzt wieder D zum Model der linearen Form, schreibt also

(4) $$Dx^2 \pm y^2 = vD + r$$

so muss sein

(5) $$\pm y^2 \equiv r \bmod D$$

Jenachdem also in der gegebenen Form das obere oder das untere Zeichen gilt, hat man die Reste der positiven oder der negativen Quadratzahlen nach dem Model D zu bilden, und wie vorhin zu verfahren.

Wäre z. B. $8x^2 - y^2$ gegeben; so sind die Reste der negativen Quadrate der aufsteigenden Zahlen nach dem Model 8 gleich 0, 4, 7, die durch jene Form darstellbaren Zahlen also $= 8v + 0, 4, 7$ und die durch dieselbe darstellbaren Primzahlen einzig $= 8v + 7$.

IV. Gehen wir jetzt zu dem allgemeineren Falle über. Soll die Determinante D der quadratischen Form (1) der Model für die lineare Form der dadurch dargestellten Zahlen sein; so ergibt sich, wenn man jene quadratische Form mit a multiplizirt und $vD + r$ für q schreibt,

$$(ax - by)^2 - Dy^2 = vaD + ar$$

also, wenn man zur Abkürzung $ax - by = z$ setzt,

(6) $$z^2 \equiv ar \bmod D$$

Um also die verschiedenen möglichen Werthe von r zu erhalten, kann man nach dem Model D erst die Reste der Quadrate der natürlichen Zahlen bilden, welche stets periodisch sind und die Werthe von z^2 vertreten. Hierauf kann man die Reste der sukzessiven Vielfachen von a bis zum $(D-1)$fachen hinauf bilden, welche die Werthe von ar vertreten. Jeder der letzteren Reste, welcher mit irgend Einem der ersteren quadratischen Reste übereinstimmt, lehrt einen zulässigen Werth von r kennen.

Dieses Verfahren ist offenbar anwendbar, gleichviel, ob es sich um eine reduzirte oder nicht reduzirte quadratische Form, ob um darzustellende prime oder nicht prime Zahlen handelt.

Man kann übrigens die Kongruenz (6), aus welcher die Werthe von r zu bestimmen sind, durch folgende Spezialisirung noch in eine zweckmässigere Gestalt bringen.

V. Zu diesem Ende bemerken wir, dass wenn die drei Zahlen a, b, c der Form (1) ein gemeinschaftliches Maass m besässen, durch jene Form überall keine Primzahlen, sondern nur Vielfache von m, also Zahlen von der Form mp dargestellt werden könnten. Um die linearen Formen derselben zu finden, kann man den Faktor m aus den Zahlen a, b, c ausscheiden und aus der übrig bleibenden quadratischen Form die lineare Form von p bestimmen, deren Multiplikation mit m alsdann auch die lineare Form der Zahlen $q = mp$ erkennen lässt.

Nehmen wir also an, die drei Zahlen a, b, c haben kein gemeinschaftliches Maass. In diesem Falle ist klar, dass sich unter den beiden äusseren Koeffizienten a und c entweder Einer findet, der zur Determinante D relativ prim ist, oder wenn jeder ein gemeinschaftliches Maass mit D hätte, doch Einer, welcher kein Vielfaches von D ist. Denn wäre jeder von beiden Koeffizienten ein Vielfaches von D, also $a = a'D$, $c = c'D$; so müssten wegen $D = b^2 + ac = b^2 + a'c'D^2$ offenbar b und D, folglich auch die drei Zahlen a, b, c ein gemeinschaftliches Maass haben, was der Voraussetzung widerspricht.

Derjenige Koeffizient, welcher der eben bezeichneten Bedingung entspricht, welcher also entweder relativ prim zu D oder doch kein Vielfaches von D ist, werde in der Form (1) vorangestellt, und vertrete darin die Stelle von a.

VI. Ist nun a relativ prim zu D; so ist es offenbar gleichgültig, ob wir in der Kongruenz (6) für z nach und nach die natürlichen Zahlen $0, 1, 2, 3 \ldots (D-1)$ oder die sukzessiven Vielfachen von a, also die Zahlen $0, a, 2a, 3a \ldots (D-1)a$ setzen, weil ja die Reste dieser Vielfachen nach dem Model D alle jene natürlichen Zahlen enthalten werden.

Setzt man aber in (6) statt der beliebig Veränderlichen z den Ausdruck az; so erhält man $a^2z^2 \equiv ar \bmod D$ und wenn man mit dem zu D relativ primen Faktor a dividirt,

(7) $$az^2 \equiv r \bmod D$$

Demnach braucht man, um die verschiedenen Werthe von r zu finden, nur die Reste des $a$fachen der sukzessiven Quadratzahlen zu nehmen.

Man sieht, dass in diesem allgemeineren Falle auch die beiden ad II. und III. erörterten Fälle mit begriffen sind.

VII. Hat dagegen a mit D das gemeinschaftliche Maass m, ohne dass a ein Vielfaches von D, also $m = D$

wäre; so sei $a = ma'$, $D = mD'$, worin nun a' und D' relativ prim sind. Ferner sei μ^2 der in dem gemeinschaftlichen Maasse m etwa vorkommende quadratische Faktor, also $m = \mu^2 m'$, sodass nun m' kein Quadrat mehr zum Faktor besitzt, und $a = \mu^2 m' a'$, $D = \mu^2 m' D'$ ist.

Führt man diese Werthe von a und D in die mit der Kongruenz (6) gleichbedeutende Gleichung $z^2 = ar + vD$ ein; so ergibt sich

$$z^2 = \mu^2 m'(a'r + vD')$$

Hiernach muss z^2 durch μ^2, also z durch μ theilbar sein. Alsdann muss aber ferner $\left(\frac{z}{\mu}\right)^2$ noch durch m', also weil m' keinen quadratischen Faktor enthält, auch $\frac{z}{\mu}$ durch m' theilbar, mithin $\frac{z}{\mu} = m'z'$ und $z = \mu m'z'$ sein. Setzt man diesen Werth für z in die obige Gleichung und dividirt durch $\mu^2 m'$; so kommt $m'z'^2 = a'r + vD'$ also

$$m'z'^2 \equiv a'r \bmod D'$$

Jetzt, wo a' und D' relativ prim sind, kann man wieder schliessen, wie ad VI., dass es gleichgültig sei, ob man für z' die natürlichen Zahlen 0, 1, 2, 3 ... oder die sukzessiven Vielfachen von a' substituire. Schreibt man demnach $a'z'$ für z' und dividirt durch den zu D' relativ primen Faktor a'; so ergibt sich

$$(8) \qquad m'a'z'^2 \equiv r \bmod D'$$

aus welcher Kongruenz die Werthe von r ebenso, wie aus (7) zu bestimmen sind. Die lineare Form der Zahlen q bezieht sich in diesem Falle auf den Model D', ist also $= vD' + r$.

VIII. Wenn man unter q nur Primzahlen verstehen will, wird man von den Werthen der Reste r alle Zahlen ausschliessen, welche mit dem Model der linearen Form ein gemeinschaftliches Maass besitzen. Man erkennt, dass hierdurch alle diejenigen Primzahlen ausgeschlossen werden würden, welche in der Determinante D der quadratischen Form (1) selbst enthalten und jederzeit durch irgend eine quadratische Form von dieser Determinante darstellbar sind.

Die eben genannten in D enthaltenen Primzahlen lassen sich übrigens leicht in folgender Weise berücksichtigen. Ist q eine solche, also $D = pq$; so wird offenbar q durch die Form

$$(9) \qquad qx^2 - py^2$$

(indem man z. B. $x = 1$, $y = 0$ setzt) dargestellt, und diese Form ist zugleich eine reduzirte.

Hiernach kann man mit Leichtigkeit die reduzirten Formen bilden, welche die verschiedenen in D enthaltenen Primzahlen

darstellen. Sind hiervon mehrere äquivalent; so stellt Eine der äquivalenten Formen eine jede der betreffenden Primzahlen dar.

IX. Schliesslich bemerken wir, dass wenn die Determinante D ein positives Quadrat d^2 ist, die reduzirten Formen, welche sämmtlich die Gestalt $2dxy + ry^2$ haben, sofort die linearen Formen der dadurch darstellbaren Primzahlen ergeben, wenn man darunter diejenigen auswählt, worin r relativ prim zu $2d$ ist, und alsdann $y = 1$ setzt. Hierdurch ergeben sich die linearen Formen für den Model $2d$ in der Gestalt $2dx + r$ und man erkennt, dass durch die betreffende Klasse von quadratischen Formen immer nur diese einzige Klasse von Primzahlen darstellbar ist.

§. 156. *Anwendung der vorstehenden Sätze auf die einfachsten quadratischen und linearen Formen der Primzahlen.*

I. Um von den Sätzen des vorhergehenden Paragraphen einige Anwendungen zu zeigen; so sei zuvörderst die Determinante $D = -1$.

In diesem Falle gibt es nach §. 124 nur die einzige reduzirte Form $x^2 + y^2$.

Da nun nach §. 153, III. jede Primzahl von der Form $4n + 1$ ein Faktor, dagegen jede Primzahl von der Form $4n + 3$ kein Faktor von $-1 - x^2$ oder $1 + x^2$ ist; so ergibt sich sofort, dass durch $x^2 + y^2$ jede Primzahl von der Form $4n + 1$, aber keine Primzahl von der Form $4n + 3$ darstellbar sei.

Nach §. 154, II. ist jede der ersteren Primzahlen auch nur in einziger Weise in der Form $x^2 + y^2$ darstellbar.

Dieser Satz, wonach jede Primzahl $4n + 1$ die Summe zweier Quadrate, und zwar nur auf einzige Weise ist, wogegen keine Primzahl $4n + 3$ diese Eigenschaft besitzt, ist schon von Fermat gefunden.

II. Nimmt man $D = -2$; so gibt es ebenfalls nur eine einzige reduzirte Form $x^2 + 2y^2$, und demnach erkennt man aus §. 153, V., dass jede Primzahl von der Form $8n + 1$ und $8n + 3$, aber keine Primzahl von der Form $8n + 5$ und $8n + 7$ durch $x^2 + 2y^2$ darstellbar sei.

III. Auch für $D = 2$ gibt es nur eine einzige reduzirte Form $x^2 - 2y^2$. Aus §. 153, IV. erhellt daher, dass jede Primzahl von der Form $8n + 1$ und $8n + 7$, aber keine Primzahl von der Form $8n + 3$ und $8n + 5$ durch $x^2 - 2y^2$ darstellbar sei.

IV. Für $D = -3$ gibt es zwei reduzirte Formen, nämlich $x^2 + 3y^2$ und $2x^2 + 2xy + 2y^2$. Durch die letztere Form werden nur paare Zahlen, also überhaupt keine Primzahlen > 2 dargestellt. Alle durch eine quadratische Form von der Determinante -3 darstellbaren Primzahlen, sind daher nur durch die erstere Form darstellbar.

Hieraus und aus §. 153, IX. folgt, dass jede Primzahl von der Form $3n + 1$ (oder, da hierin n jedenfalls paar sein wird, von der Form $6n + 1$), aber keine Primzahl von der Form $3n + 2$ (oder, da hierin n jedenfalls unpaar sein wird, von der Form $6n + 5$) durch $x^2 + 3y^2$ darstellbar sei.

Die Primzahl 3 selbst gehört ebenfalls der Form $x^2 + 3y^2$ an.

V. Für $D = 3$ gibt es die beiden reduzirten Formen $x^2 - 3y^2$ und $3x^2 - y^2$. Darstellbar durch irgend Eine dieser beiden Formen sind nach §. 153, VIII. nur die Primzahlen, welche gleichzeitig den linearen Formen $3w + 1$ und $4n + 1$, sowie diejenigen, welche gleichzeitig den linearen Formen $3w + 2$ und $4n + 3$ entsprechen, also nur die Primzahlen von der Form $12w + 1$ oder von der Form $12w + 11$.

Untersuchen wir nun die Reste r der Form $x^2 - 3y^2$ nach §. 155, II.; so sind dieselben $\equiv x^2 \bmod 3$, also $= 0$ und 1. Demnach würden durch diese quadratische Form nur Primzahlen von der linearen Form $3v + 1$ oder von den Formen $12v + 1$, 4, 7, 10 darstellbar sein. Von allen diesen stimmt nur die Form $12v + 1$ mit der Einen der linearen Formen überein, welchen alle in Rede stehenden Primzahlen nach dem Vorhergehenden entsprechen müssen.

Was die zweite Form $3x^2 - y^2$ betrifft; so sind deren Reste r nach §. 155, III. $\equiv -y^2 \bmod 3$ also $= 0$ oder 2. Demnach würden hier die Primzahlen von der Form $3v + 2$ oder von den Formen $12v + 2$, 5, 8, 11 in Betracht kommen. Hiervon stimmt nur die Form $12v + 11$ mit der früheren überein, welcher alle darstellbaren Primzahlen entsprechen müssen.

Hieraus folgt nun, dass alle Primzahlen $12v + 1$ ausschliesslich der Form $x^2 - 3y^2$ und alle Primzahlen $12v + 11$ ausschliesslich der Form $3x^2 - y^2$ angehören, und dass Primzahlen von den Formen $12v + 5$ und $12v + 7$ überhaupt durch keine quadratische Form von der Determinante 3 darstellbar seien.

Die Primzahl 3 selbst gehört der letzteren, nicht der ersteren Form an.

§. 157. ***Die binomischen Kongruenzen höherer Grade von der Form*** $x^n \equiv 1$. — ***Primitive Wurzeln dieser Kongruenzen.***

I. **Für gewisse höhere Untersuchungen in der Theorie der Zahlen haben die binomischen Kongruenzen von der Form**

$$x^n \equiv 1 \mod p \tag{1}$$

worin der Model p eine Primzahl sein soll, eine besondere Wichtigkeit. Diese Kongruenz $n$ten Grades kann bekanntlich höchstens n verschiedene, d. h. nach dem Model p nicht kongruente Wurzeln haben, von welchen man immer voraussetzen kann, dass sie positiv und kleiner als p seien (§. 146, I.).

Die genaue Anzahl der verschiedenen Wurzeln der Kongruenz (1) findet man, wenn man nach §. 146, VII. das grösste gemeinschaftliche Maass zwischen den beiden Funktionen

$$x^n - 1 \quad \text{und} \quad x^{p-1} - 1 \tag{2}$$

sucht.

Besitzen nun allgemein die Exponenten von x in zwei Binomen der vorstehenden Art das grösste gemeinschaftliche Maass r, hätte man also die beiden Binome

$$x^{rs} - 1 = (x^r)^s - 1$$
$$x^{rt} - 1 = (x^r)^t - 1$$

so erkennt man nicht bloss sofort, dass $x^r - 1$ ein gemeinschaftliches Maass beider Binome ist, sondern das bekannte algebraische Divisionsverfahren lehrt auch leicht, dass $x^r - 1$ das grösste gemeinschaftliche Maass jener beiden Binome ist.

Hieraus folgt, dass wenn der Exponent n der Kongruenz (1) relativ prim zur Zahl $p - 1$ ist, wenn also n und $p - 1$ nur das grösste gemeinschaftliche Maass 1 besitzen, das grösste gemeinschaftliche Maass der beiden Binome (2) $x - 1$ ist, dass also in diesem Falle die Kongruenz (1) nur die einzige Wurzel $x = 1$, welche positiv und $< p$ ist, oder allgemein die Wurzel $x \equiv 1 \mod p$ enthält.

So würde z. B. die Kongruenz $x^3 \equiv 1 \mod 5$ nur die Wurzel 1 besitzen, da 3 und 4 relativ prim sind.

Was nun aber eine Kongruenz von der Form (1) betrifft, deren Exponent $n = rs$ mit der Zahl $p - 1 = rt$ das grösste gemeinschaftliche Maass r besitzt; so hat jene Kongruenz keine anderen Wurzeln, als die Kongruenz $x^r \equiv 1$, worin r ein Faktor von $p - 1$ ist.

So hat z. B. die Kongruenz $x^8 \equiv 1 \mod 13$, wofür 8 und 12 das grösste gemeinschaftliche Maass 4 besitzen, keine anderen Wurzeln, als die Kongruenz $x^4 \equiv 1$.

Demnach können die Untersuchungen über die Wurzeln der Kongruenzen von der Form (1) auf die Fälle beschränkt werden, wo der Exponent n ein Faktor von $p - 1$ ist.

II. Eine solche Kongruenz hat offenbar ebenso viel verschiedene Wurzeln, als ihr Exponent n Einheiten. Sind diese Wurzeln $a, b, c \ldots$; so ist klar, dass jede Potenz irgend Einer dieser Wurzeln, oder der kleinste Rest einer jeden Potenz von einer solchen Wurzel die Kongruenz (1) erfüllt, also wiederum eine Wurzel der Letzteren ist. Hätte man also

$$\begin{array}{lll} a \equiv R_1 & b \equiv S_1 & c \equiv T_1 \\ a^2 \equiv R_2 & b^2 \equiv S_2 & c^2 \equiv T_2 \\ a^3 \equiv R_3 & b^3 \equiv S_3 & c^3 \equiv T_3 \\ \vdots & \vdots & \vdots \end{array}$$

so wären alle mit $R, S, T \ldots$ bezeichneten Zahlen Wurzeln der Kongruenz (1). Diese Zahlen können natürlich nicht sämmtlich verschieden sein, da ja die gegebene Kongruenz überhaupt nur n verschiedene Wurzeln besitzt. Vielmehr bilden sowol die Zahlen R, wie die S, T etc. Perioden, deren letztes Glied immer $= 1$ ist, während die übrigen Glieder verschieden von einander und von 1 sind (§. 142).

Keine dieser Perioden kann mehr als n Glieder enthalten. Wol aber kann eine solche Periode weniger als n und auch genau n Glieder besitzen.

Besässe eine Periode, z. B. die der R, weniger als n, etwa m Glieder; so kann nach §. 141 m nur ein Faktor von n sein, und es ist klar, dass alsdann die Zahl a auch die Wurzel einer Kongruenz $x^m \equiv 1$ ist, deren Exponent $m < n$ und zwar ein Faktor von n ist. **Dieser Fall kann also, wenn der Exponent n der Kongruenz (1) eine Primzahl ist, nur für die einzige Wurzel a eintreten, welche $= 1$ ist, und für welche die fragliche Periode immer nur aus einem einzigen Gliede besteht. Für jede andere der übrigen $n - 1$ Wurzeln $b, c \ldots$ muss dann die Periode der S, der T u. s. w. genau n verschiedene Glieder besitzen.**

Die letztere Erscheinung, wo die Periode der Grössen R oder S oder $T \ldots$ genau n Glieder enthält, kann übrigens auch für diese und jene der Wurzeln $a, b, c \ldots$ selbst dann eintreten, wenn der Exponent n keine Primzahl ist. Eine Wurzel der letzteren Art besitzt alsdann folgende zwei bemerkenswerthe Eigenschaften: Sie gehört keiner Kongruenz von der Form (1) an, deren Exponent kleiner als n wäre, und die Reste ihrer sukzessiven Potenzen $a, a^2, a^3 \ldots$ liefern alle Wurzeln $a, b, c \ldots$ der gegebenen Kongruenz (1). Man erkennt auch, dass die Eine dieser beiden Eigenschaften die andere bedingt. Diejenigen der Wurzeln $a, b, c \ldots$, welche die vorstehenden Eigenschaften besitzen, nennt man primitive Wurzeln der Kongruenz (1). **Man sagt auch, eine Zahl a, welche nach vorstehender Erklärung eine primitive Wurzel**

der Kongruenz (1) ist, von welcher also keine niedrigere, als die $n$te Potenz kongruent 1 ist, gehöre zum Exponenten n.

III. Dass die Kongruenz (1) stets primitive Wurzeln haben müsse, erkennt man durch folgende Betrachtung.

Für den Fall, dass der Exponent n eine Primzahl ist, weiss man schon aus dem Obigen, dass mit Ausschluss der Wurzel 1 alle übrigen $n-1$ Wurzeln primitiv sind.

Setzen wir jetzt voraus, n sei eine Potenz einer Primzahl, also $=r^\alpha$. Wäre nun unter allen n Wurzeln keine primitive vorhanden, gehörten also alle diese Wurzeln Kongruenzen an, deren Exponenten kleiner als n und Faktoren von n wären; so könnten die Exponenten dieser niedrigeren Kongruenzen nur die Werthe $r, r^2, r^3 \ldots r^{\alpha-1}$ haben. Die Wurzeln aller Kongruenzen, deren Exponenten $r, r^2, r^3 \ldots r^{\alpha-2}$ sind, kommen aber offenbar in der letzten Kongruenz vor, deren Exponent $r^{\alpha-1}$ ist. Diese Kongruenz besitzt jedoch nur $r^{\alpha-1}$ Wurzeln; es müssen also unter den $n=r^\alpha$ Wurzeln der gegebenen Kongruenz nothwendig primitive vorkommen. Da die Anzahl der nicht primitiven Wurzeln in diesem Falle $=r^{\alpha-1}$ ist; so ist die Anzahl der primitiven Wurzeln $=r^\alpha - r^{\alpha-1} = (r-1)r^{\alpha-1}$ $= \frac{(r-1)n}{r}$.

Endlich sei der Exponent der Kongruenz (1) eine beliebige zusammengesetzte Zahl von der Form $n=rst\ldots$, worin $r, s, t\ldots$ Potenzen verschiedener Primzahlen seien. Ist dann resp. $\alpha, \beta, \gamma\ldots$ eine primitive Wurzel der Kongruenz $x^r\equiv 1$, $x^s\equiv 1$, $x^t\equiv 1\ldots$; so kann man zeigen, dass das Produkt $\alpha\beta\gamma\ldots$ oder dessen kleinster Rest eine primitive Wurzel der gegebenen Kongruenz sei.

Denn zunächst leuchtet ein, dass

$$(\alpha\beta\gamma\ldots)^{rst\ldots}\equiv 1$$

dass also jenes Produkt $\alpha\beta\gamma\ldots$ überhaupt eine Wurzel der gegebenen Kongruenz ist. Wäre dasselbe nun keine primitive Wurzel; so müsste es zugleich die Wurzel einer Kongruenz sein, deren Exponent m ein Faktor von $rst\ldots$ ist, sodass man allgemein $r=r'r''$, $s=s's''$, $t=t't''\ldots$ und $m=r's't'\ldots$ setzen kann, worin mindestens Einer der Faktoren $r', s', t'\ldots$ kleiner als der korrespondirende von $r, s, t\ldots$ ist. Wäre z. B. $r'<r$; so beachte man, dass wenn

$$(\alpha\beta\gamma\ldots)^{r's't'\ldots}\equiv 1 \text{ ist, auch}$$

$$(\alpha\beta\gamma\ldots)^{r's's''t't''\ldots} = (\alpha\beta\gamma\ldots)^{r'st\ldots}\equiv 1 \text{ sein wird.}$$

Nun hat man offenbar ohne Weiteres auch für das Produkt $\beta\gamma\ldots$, von welchem die Zahl a ausgeschlossen ist,

$$(\beta\gamma\ldots)^{r's t\ldots} \equiv 1$$

mithin

$$(\alpha\beta\gamma\ldots)^{r's t\ldots} \equiv (\beta\gamma\ldots)^{r's t\ldots}$$

und wenn man diese Kongruenz durch $(\beta\gamma\ldots)^{r's t\ldots}$ dividirt,

$$\alpha^{r'} \equiv 1$$

Dieses Resultat widerspricht der Voraussetzung, wonach α eine primitive Wurzel der Kongruenz vom Exponenten r sein soll. Es muss also $\alpha\beta\gamma\ldots$ eine primitive Wurzel der gegebenen Kongruenz sein.

IV. Die Anzahl der primitiven Wurzeln der Kongruenz $x^n \equiv 1$ ist ebenso gross, als die Anzahl der Zahlen, welche $< n$ und relativ prim zu n sind (wobei die Zahl 1 als unter die zu n relativ primen mitgerechnet wird).

Denn ist a eine primitive Wurzel; so können die n ersten Potenzen von a, also $a, a^2, a^3 \ldots a^n$ als die Vertreter der n Wurzeln der gegebenen Kongruenz angesehen werden, indem die letzte Potenz a^n die Wurzel 1 vertritt. Jede höhere Potenz von a entspricht einer Wurzel, welche mit irgend Einer der vorstehenden identisch ist, und zwar hat man allgemein $a^{m+s} \equiv a^s$, sodass die Wurzel 1 nur durch diejenigen Potenzen vertreten wird, deren Exponenten Vielfache von n sind.

Ist nun s irgend Eine zu n relativ prime Zahl aus der Reihe 1, 2, 3 ... n, und bildet man von der Wurzel a^s die ersten n Potenzen $a^s, a^{2s}, a^{3s} \ldots a^{ns}$, welche offenbar sämmtlich Wurzeln der gegebenen Kongruenz darstellen; so kann hierunter nur die letzte, und keine andere, wie etwa a^{ts} die Wurzel 1 vertreten. Denn sonst müsste ts ein Vielfaches von n, also, da s und n relativ prim sein sollen, t ein Vielfaches von n sein.

Hiernach ist von den sukzessiven Potenzen von a^s die $n$te Potenz a^{ns} die niedrigste, welche $\equiv 1$ ist. Mithin sind die Reste aller dieser Potenzen oder die dadurch dargestellten Wurzeln der Kongruenz (1) sämmtlich verschieden (§. 142), d. h. a^s ist ebenfalls eine primitive Wurzel dieser Kongruenz.

V. Das Vorstehende lehrt zugleich, wie sich alle übrigen primitiven Wurzeln der Kongruenz (1) ergeben, wenn eine einzige a bekannt ist. Bezeichnen nämlich $r, s, t\ldots$ die Zahlen, welche $< n$ und relativ prim zu n sind, wobei man auch den Werth $r = 1$ mitrechnet; so sind die gesuchten primitiven Wurzeln die Reste der Potenzen

$$a^r,\ a^s,\ a^t \ldots$$

So ist z. B. 5 eine primitive Wurzel der Kongruenz $x^4 \equiv 1 \bmod 13$. Demnach sind, da es nur die beiden Zahlen 1 und 3 giebt,

welche < 4 und relativ prim zu 4 sind, alle primitiven Wurzeln jener Kongruenz die Reste der beiden Potenzen 5^1 und 5^3 d. i. 5 und 8.

VI. Wenn der Exponent n der Kongruenz (1) den Werth $p-1$ hat; so nennt man die primitiven Wurzeln der in mancher Beziehung wichtigen Kongruenz

(3) $$x^{p-1} \equiv 1 \; mod \, p$$

kurzweg die primitiven Wurzeln von p oder wie wir uns lieber ausdrücken würden, die primitiven Wurzeln **nach** p.

VII. Aus dem Umstande, dass jede Kongruenz wie die vorstehende (3) primitive Wurzeln hat, lässt sich der Wilsonsche Lehrsatz (§. 144) leicht auf folgende Weise ableiten. Ist a eine solche primitive Wurzel; so kommen unter den Resten der ersten $p-1$ Potenzen von a alle Zahlen $1, 2, 3 \ldots (p-1)$ vor. Multiplizirt man also alle diese Potenzen miteinander; so kommt

$$a^{\frac{p(p-1)}{2}} \equiv 1 \,.\, 2 \,.\, 3 \ldots (p-1)$$

und da nun $n = p-1$, $m = 1$, also nach §. 145, III., $a^{\frac{p-1}{2}} \equiv (-1)^m \equiv -1$, folglich $a^{\frac{p(p-1)}{2}} = \left(a^{\frac{p-1}{2}}\right)^p \equiv (-1)^p \equiv -1$ ist,

$$1 \,.\, 2 \,.\, 3 \ldots (p-1) \equiv -1$$

VIII. Dem Ende dieses Werkes haben wir eine aus dem 9ten Bande von Crelles Journale für Mathematik entlehnte Tafel der primitiven Wurzeln der Kongruenz (1) für die Primzahlenwerthe des Models p von 2 bis 67 und für alle Werthe des Exponenten n, welche Faktoren von $p-1$ sind, angehängt.

§. 158. *Die Indizes der Zahlen.*

I. Wenn B irgend eine primitive Wurzel nach der Primzahl p, also eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \; mod \, p$ ist; so denke man sich alle durch p nicht theilbare Zahlen, wie z. B. die Zahl a, auf die Zahl B als Basis eines Potenzensystems bezogen, sodass die Exponenten e ermittelt sind, für welche

(1) $$B^e \equiv a \; mod \, p$$

ist. Der Exponent e heisst dann nach Gauss der Index von a, und wir schreiben

(2) $$ind \, a = e$$

II. Jede Zahl a besitzt zwar unendlich viele verschiedene Indizes; dieselben unterscheiden sich jedoch nur durch Viel-

fache der Zahl $p-1$ voneinander oder sind sämmtlich nach dem Model $p-1$ kongruent.

Denn wäre nach dem Model p zugleich $B^e \equiv a$ und $B^f \equiv a$ und $f > e$; so hätte man

$$B^f - B^e = B^e(B^{f-e} - 1) \equiv 0$$

folglich auch, da $B^e \equiv a$ und a zum Model p relativ prim ist, $B^{f-e} - 1 \equiv 0$ oder $B^{f-e} \equiv 1$, was, da B eine primitive Wurzel nach p darstellt, nur möglich ist, wenn $f-e$ ein Vielfaches von $p-1$ oder $f \equiv e \mod (p-1)$ ist.

Demnach gelten die nach dem Model $p-1$ kongruenten Indizes e für gleichbedeutend, sowie die nach dem Model p kongruenten Zahlen a für gleichbedeutend angesehen werden können.

III. Für die Indizes gelten einige leicht zu erweisende Sätze, welche denen der Logarithmen analog sind. Es ist nämlich:

der Index eines Produkts kongruent der Summe der Indizes der Faktoren nach dem Model $p-1$, also

(3) $$ind\, abc \equiv ind\, a + ind\, b + ind\, c \quad mod\,(p-1)$$

IV. Ferner ist der Index der Potenz einer Zahl kongruent dem Produkte aus dem Index dieser Zahl und dem Exponenten der Potenz nach dem Model $p-1$, nämlich

(4) $$ind\, a^n \equiv n\, ind\, a \quad mod\,(p-1)$$

V. Aus Vorstehendem ist klar, dass wenn man die Indizes aller Primzahlen kennt, welche kleiner als der Model p sind, man daraus leicht den Index jeder Zahl a bestimmen kann, dieselbe sei grösser oder kleiner als p, zusammengesetzt oder nicht.

Denn ist $a > p$; so kann zunächst für a sein kleinster positiver Rest nach dem Model p genommen werden.

Ist dieser Rest, welcher kleiner als p ist, $= b^m c^n \ldots$, worin $b, c \ldots$ Primzahlen $< p$ sind; so ist

(5) $$ind\, a \equiv m\, ind\, b + n\, ind\, c + \ldots \quad mod\,(p-1)$$

VI. Am Ende dieses Werkes haben wir die den *Disq. arithm.* von Gauss entlehnte Tafel der Indizes eingeschaltet. Dieselbe bildet eigentlich eine Zusammenstellung von Tabellen, indem sich jede Horizontalreihe auf einen besonderen Model bezieht. Man findet darin für alle Primzahlen unter 100, als Model, die Indizes aller Primzahlen, welche kleiner sind, als der betreffende Model. Die jeder Horizontalreihe zu Grunde liegende Basis ist gleichfalls angemerkt.

So ist z. B. für den Model $p = 19$ (indem als Basis B die primitive Wurzel 10 der Kongruenz $x^{18} \equiv 1 \bmod 19$ angenommen ist).

$ind\ 7 = 12$
$ind\,22 = ind\ 3 = 5$
$ind\ 6 = ind\ 2 \,.\, 3 \equiv ind\ 2 + ind\ 3 \equiv 17 + 5 \equiv 22 \bmod 18 = 4$

VII. Aus einer solchen Tafel kann man zwar für jede gegebene Zahl den zugehörigen Index bestimmen; will man aber für einen gegebenen Index die zugehörige Zahl finden; so kann Dies ohne Weiteres nur dann geschehen, wenn der gegebene Index selbst in der Tafel vorkommt. So ist z. B. die für den Model 19 und die Basis 10 dem Index 6 angehörige Zahl gleich 11.

Kommt aber der gegebene Index nicht in der Tafel vor; so muss man, wenn keine für diesen Zweck besonders eingerichtete Tafel vorliegt, sich damit begnügen, zu versuchen, wie sich der gegebene Index aus den in der Tafel vorkommenden Indizes durch Addition oder Vervielfältigung oder Beides zugleich darstellen lasse. Sollte z. B. für den Model 19 und die Basis 10 der Index einer Zahl gleich 11 sein; so findet sich nach einigen Versuchen, dass $17 + 12 = 29 \equiv 11 \bmod 18$, dass also, wenn x die gesuchte Zahl bezeichnet, $ind\, x = ind\ 2 + ind\ 7 \equiv ind\ 14$, folglich $x = 14$ ist.

Das letztere Verfahren ist freilich etwas umständlich. Es erleichtert sich aber, besonders wenn man für Ein und denselben Model mehrfache Rechnungen auszuführen hat, dadurch, dass man die für diesen Model gültige Reihe der Indizes im Voraus für alle unterhalb jenes Models liegenden Zahlen erweitert, was nach den obigen Sätzen sehr leicht geschehen kann, wenn man die Zusammensetzung der fehlenden Zahlen aus ihren Primfaktoren berücksichtigt.

Um z. B. auf diese Weise die Reihe für den Model 19 zu vervollständigen, erhält man

Zahlen	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18
Indizes	0.	17.	5.	16.	2.	4.	12.	15.	10.	1.	6.	3.	13.	11.	7.	14.	8.	9

Aus dieser vervollständigten Tabelle würde man sofort erkannt haben, dass die im vorhergehenden Beispiele gesuchte Zahl, deren Index $= 11$ sein sollte, den Werth 14 besitzt.

§. 159. *Auflösung der binomischen Kongruenzen mit Hülfe der Indizes.*

I. Mit Hülfe der im vorstehenden Paragraphen beschriebenen und für den gegebenen Model vervollständigten Tafel der Indizes ist es leicht, die binomischen Kongruenzen aller

Grade, deren Model eine Primzahl ist, zu lösen, wenn sie überhaupt lösbar sind.

Für die Kongruenz ersten Grades

(1) $$bx \equiv a \, mod \, p$$

hat man $ind\, b + ind\, x \equiv ind\, a \quad mod\,(p-1)$ also

(2) $$ind\, x \equiv ind\, a - ind\, b \quad mod\,(p-1)$$

Um also die Wurzel x der Kongruenz (1) zu erhalten, subtrahirt man vom Index der Zahl a den Index der Zahl b und sucht die Zahl x, welcher diese Differenz als Index zukommt.

Wäre z. B.

$$477x \equiv 195 \, mod\, 19 \quad \text{oder in kleinsten Zahlen}$$
$$2x \equiv 5 \, mod\, 19$$

zu lösen; so hat man

$$ind\, x \equiv ind\, 5 - ind\, 2 \equiv 2 - 17 \equiv -15 \equiv 3 \, mod\, 18$$

folglich $x = 12$ und allgemein $x \equiv 12 \, mod\, 19$.

II. Für die binomische Kongruenz $n$ten Grades von der Form

(3) $$x^n \equiv a \, mod\, p$$

hat man

(4) $$n\, ind\, x \equiv ind\, a \quad mod\,(p-1)$$

Die letztere Kongruenz (4) ist in Beziehung zu der Grösse $ind\, x$ eine Kongruenz ersten Grades nach dem Model $p-1$, welche nach bekannten Regeln für die Unbekannte $ind\, x$ zu lösen ist. Alle hierdurch für $ind\, x$ sich ergebenden Werthe, welche $< p-1$ sind, führen zu ebenso viel verschiedenen Werthen für x selbst oder zu Auflösungen der Kongruenz (3), und es ist klar, dass die Kongruenz (3) dann und auch nur dann unmöglich sein wird, wenn die Kongruenz (4) es ist.

Wäre z. B.

$$x^{15} \equiv 11 \, mod\, 19$$

zu lösen; so hat man

$$15\, ind\, x \equiv ind\, 11 \, mod\, 18 \quad \text{also}$$
$$15\, ind\, x \equiv 6 \, mod\, 18$$

Diese Kongruenz liefert für $ind\, x$ die drei Auflösungen 4, 10, 16, welche kleiner sind, als 18. Jenen drei Indizes entsprechen aber als gesuchte Auflösungen der gegebenen Kongruenz die drei Werthe $x = 6, 9, 4$ oder allgemeiner $x \equiv 6, 9, 4 \, mod\, 19$.

III. Aus der Beschaffenheit der Kongruenz (4) lassen sich leicht einige wichtige Sätze über die Anzahl der möglichen Wurzeln der Kongruenz (3) ableiten.

Wenn der Exponent n der gegebenen Kongruenz (3) ein Faktor von $p-1$ ist, wenn man also $p-1=mn$ hat; so ist diese Kongruenz dann aber auch nur dann möglich, wenn n auch ein Faktor von $ind\,a$ ist, wenn man also $ind\,a=nv$ hat. Ist Letzteres aber der Fall, also $B^{nv}\equiv a \mod p$; so ist auch, indem man diese Kongruenz auf den Grad m erhebt und dabei beachtet, dass $B^{mnv}=(B^{p-1})^v$ und $B^{p-1}\equiv 1 \mod p$ ist,

(5) $$a^m\equiv 1 \mod p$$

Umgekehrt kann man behaupten, dass wenn a die Kongruenz (5) erfüllt, auch jederzeit die Kongruenz (3) lösbar ist, wobei jedoch vorausgesetzt wird, dass $mn=p-1$ sei. Denn setzt man $B^e\equiv a \mod p$; so ist wegen (5) auch $B^{em}\equiv 1 \mod p$. Da aber die Basis B eine primitive Wurzel der Kongruenz $x^{p-1}\equiv 1 \mod p$ ist; so können nur diejenigen Potenzen von B, deren Exponenten Vielfache von $p-1$ sind, $\equiv 1$ sein. Hiernach ist em ein Vielfaches von $p-1$ oder von mn, folglich n ein Faktor von e oder vom Index der Zahl a; mithin die Kongruenz (4) und demnach auch die Kongruenz (3) möglich.

IV. Nach demselben Prinzipe, nach welchem in §. 146, VIII. die quadratischen Reste benannt wurden, nennt man eine Grösse a, welche einem Kubus, einem Biquadrate oder allgemein einer $n$ten Potenz irgend einer anderen Grösse x nach dem Model p kongruent ist, für welche also die Kongruenz $x^3\equiv a$, $x^4\equiv a$ oder allgemein $x^n\equiv a \mod p$ lösbar ist, resp. einen kubischen, einen biquadratischen oder allgemein einen Rest $n$ten Grades nach p.

Das sub III. gefundene Resultat lässt sich also für den Fall, dass der Model p eine Primzahl und n ein Faktor von $p-1$ sei, auch so ausdrücken. Eine Grösse a ist dann und auch nur dann ein Rest $n$ten Grades nach p, wenn

$$a^{\frac{p-1}{n}}\equiv 1 \mod p$$

ist. Hiervon ist das in §. 147 ausgesprochene Gesetz der quadratischen Reste offenbar nur ein spezieller Fall.

V. Unter den sub III. und IV. gemachten Voraussetzungen hat aber die Kongruenz (3) nicht bloss Eine, sondern n verschiedene Wurzeln. Denn die Kongruenz (4), welche sich jetzt auf

$$ind\,x\equiv\frac{ind\,a}{n} \quad \mod \frac{p-1}{n}$$

reduzirt, liefert einen Werth von $ind\,x$, welcher $<\frac{p-1}{n}$ ist, also n Werthe, welche $<p-1$ sind.

Nachdem Eine Wurzel b der Kongruenz (3) gefunden ist, kann man, wenn c eine primitive Wurzel der Kongruenz $x^n \equiv 1 \bmod p$ bezeichnet, alle n Wurzeln der Kongruenz (3) durch b, bc, bc^2, $bc^3 \ldots bc^{n-1}$ darstellen.

VI. Wenn der Exponent n eine in $p-1$ nicht enthaltene Primzahl ist; so hat die Kongruenz (4) und mithin die Kongruenz (3) stets eine Auflösung, aber auch nur eine einzige.

VII. Wenn der Exponent n mit der Zahl $p-1$ das grösste gemeinschaftliche Maass r besitzt, also $n = rs$ und $p-1 = rt$ ist; so verlangt die Möglichkeit der Kongruenz (4), **dass r ein Faktor von $ind\, a$ sei. Ist Dies der Fall; so ist die Kongruenz (4) und folglich auch die Kongruenz (3) lösbar, sonst nicht; und dieselbe besitzt im ersteren Falle r verschiedene Wurzeln.**

Die Bedingung, dass r ein Faktor des Index von a sei, führt, wenn man demzufolge $B^{rw} \equiv a \bmod p$ also auch $B^{rtw} \equiv a^t \bmod p$ setzt, und beachtet, dass $B^{rt} = B^{p-1} \equiv 1$ ist, zu der gleichbedeutenden Bedingung, dass

$$(6) \qquad a^t \equiv 1 \bmod p$$

sei.

Der letztere ist der allgemeinere Fall und lehrt, dass wenn r das grösste gemeinschaftliche Maass von n und $d-1$, ferner $rt = p-1$ ist, a nur dann ein Rest $n$ten Grades nach p ist, wenn man $a^t \equiv 1$ hat.

Ist von der Kongruenz (3) Eine Wurzel b bekannt, und bezeichnet c eine primitive Wurzel der Kongruenz $x^r \equiv 1 \bmod p$; so sind sämmtliche r verschiedene Wurzeln der Kongruenz (3) dargestellt durch b, bc, bc^2, $bc^3 \ldots bc^{r-1}$.

VIII. Was endlich die allgemeinere Form

$$(7) \qquad bx^n \equiv a \bmod p$$

der binomischen Kongruenz betrifft; so reduzirt sich die Lösung der Letzteren erst auf die Lösung der Kongruenz ersten Grades

$$(8) \qquad by \equiv a \bmod p$$

und alsdann auf die Lösung der Kongruenz

$$(9) \qquad x^n \equiv y \bmod p$$

Will man die Indizes zu Hülfe nehmen; so hat man sofort $ind\, b + n\, ind\, x \equiv ind\, a \bmod (p-1)$, also

$$(10) \qquad n\, ind\, x \equiv ind\, a - ind\, b \quad \bmod (p-1)$$

welche Kongruenz ersten Grades für $ind\, x$ zu lösen ist.

Wäre z. B.

$$3x^5 \equiv 7 \bmod 19$$

zu lösen; so hat man

$$5\,ind\,x \equiv ind\,7 - ind\,3 \equiv 12 - 5 \equiv 7\;mod\,18$$

also $ind\,x = 5$ und demnach $x = 3$ oder allgemeiner $x \equiv 3\,mod\,19$.

IX. Wenn der Model p in der Kongruenz (7) keine Primzahl, sondern allgemein von der Form $p^\alpha q^\beta \ldots$ ist, worin p, $q \ldots$ verschiedene Primzahlen darstellen; so muss die gegebene Kongruenz offenbar für jeden Primfaktor p, $q \ldots$ des Models, als Model genommen, lösbar sein. Ebenso muss sie für jede der Zahlen p^α, $q^\beta \ldots$, als Model genommen, lösbar sein, und wenn sie Dies ist, ist sie auch für den Model $p^\alpha q^\beta \ldots$ lösbar. Lös't man dieselbe für jeden der Model p^α, $q^\beta \ldots$ auf (was mit Hülfe einer Indizes-Tafel geschehen kann, in welcher auch die Potenzen der Primzahlen zu Modeln angenommen sind) und sind x, $y \ldots$ die speziellen Auflösungen für jene Model, also $x + vp^\alpha$, $y + wq^\beta \ldots$ die allgemeinen Auflösungen für jene Model; so liefern diejenigen Werthe von X, für welche man

(11) $$X = x + vp^\alpha = y + wq^\beta = \ldots$$

hat, die Auflösungen der gegebenen Kongruenz nach dem Model $p^\alpha q^\beta \ldots$

Siebenter Abschnitt.

Auflösung der homogenen Gleichungen vom zweiten Grade mit drei Unbekannten sowol in ganzen, wie in rationalen Zahlen und der allgemeinen Gleichungen vom zweiten Grade mit zwei Unbekannten in rationalen Zahlen.

Homogene Gleichungen mit drei Unbekannten in ganzen Zahlen.

§. 160. *Auflösung der einfachsten Gleichungen dieser Art.*

Unter einer homogenen Gleichung mit mehreren Unbekannten von irgend einem Grade n versteht man eine solche, in welcher jedes Glied n Dimensionen in Beziehung zu den Unbekannten enthält.

Demnach würde die allgemeinste Form einer homogenen Gleichung vom zweiten Grade mit 3 Unbekannten x, y, z folgende sein: $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$.

Bei der Lösung dieser Gleichungen steigen wir von den einfacheren Fällen zu den zusammengesetzteren auf.

I. Zuerst sei die Gleichung

(1) $$x^2 - y^2 = z^2$$

gegeben, welche in der Form

$$x^2 = y^2 + z^2$$

die Aufgabe enthält, zwei ganze Zahlen y und z zu finden, deren Quadratsumme wiederum ein Quadrat ist. Die Gl. (1) lässt sich auch so schreiben:

(2) $$(x + y)(x - y) = z^2$$

Die Faktoren der rechten Seite z^2 dieser Gleichung müssen sich also über die beiden Faktoren $x + y$ und $x - y$ der linken

Seite dieser Gleichung in irgend einer Weise vertheilen. Da die rechte Seite ein vollkommenes Quadrat ist, also alle Faktoren derselben zusammengenommen ein Quadrat bilden müssen; so kann die eben bezeichnete Vertheilung in grösster Allgemeinheit so gedacht werden, dass Ein Theil der quadratischen Faktoren von z^2 auf $x+y$, ferner ein anderer Theil jener quadratischen Faktoren auf $x-y$ kommt, dass aber von dem dritten Theile aller jener quadratischen Faktoren die Eine Wurzel auf $x+y$ und die andere Wurzel auf $x-y$ kommt.

Demnach kann man z als das Produkt dreier ganzer Zahlen u, v, w, also als

(3) $$z = uvw$$

darstellen, und indem man $z^2 = u^2v^2w^2 = (uv^2)(uw^2)$ schreibt,

(4) $$x + y = uv^2$$

(5) $$x - y = uw^2$$

setzen. Hieraus ergibt sich die Auflösung der gegebenen Gleichung (1) in der Form

(6) $$x = \frac{u(v^2+w^2)}{2}, \quad y = \frac{u(v^2-w^2)}{2}, \quad z = uvw$$

Damit diese Ausdrücke nicht bloss für z, sondern auch für x und y ganze Zahlen liefern, können u, v, w nicht völlig willkürlich bleiben. Es sind jedoch leicht die Bedingungen zu übersehen, welchen diese Grössen unterworfen werden müssen. Es muss nämlich entweder v^2+w^2 und v^2-w^2 oder u eine paare Zahl sein. Man kann also entweder v und w paar und u beliebig oder v und w unpaar und u beliebig oder v und w beliebig und u paar annehmen, um ganze Auflösungen zu erhalten.

Wollte man Ein für alle Mal statt u eine paare Zahl $2u'$ einführen; so würden die Formeln

$$x = u'(v^2+w^2), \quad y = u'(v^2-w^2), \quad z = 2u'vw$$

zwar für alle willkürliche Werthe von u', v, w ganze Zahlen ergeben. Allein dessenungeachtet stellen diese Ausdrücke die Auflösung der gegebenen Gleichung (1) nicht in grösster Allgemeinheit dar, was man schon daraus erkennt, dass hiernach z stets paar sein würde, was gar nicht nothwendig ist.

Man hat also als allgemeine Auflösung die Ausdrücke (6) beizubehalten und darin für v, w oder u in der angegebenen Weise zulässige Werthe zu substituiren.

Die Natur der Gl. (1) lehrt, dass man jeden Werth von irgend Einer der drei Grössen auch mit entgegengesetztem Zeichen nehmen kann. Dasselbe lehrt die Auflösung (6). Denn nimmt man darin für u den entgegengesetzten Werth;

so kehren sich die Zeichen von x, y, z zugleich um. Nimmt man v oder w mit entgegengesetzten Zeichen; so kehrt sich das Zeichen von z allein um. Verwechselt man die Werthe von v und w miteinander; so kehrt sich das Zeichen von y allein um. Hiernach kann man leicht bewirken, dass von den Grössen x, y, z entweder Eine oder zwei oder alle drei entgegengesetzte Zeichen erhalten.

II. Jetzt sei gegeben

(7) $$x^2 - y^2 = cz^2$$

oder auch

$$x^2 = y^2 + cz^2$$

worin c eine beliebige positive oder negative ganze Zahl darstelle. Zerlegt man c auf irgend eine Weise in zwei Faktoren p, q, sodass man

(8) $$pq = c$$

hat, und schreibt auch hier wieder $z = uvw$; so hat man

$$(x+y)(x-y) = cz^2 = pqu^2v^2w^2 = (puv^2)(quw^2)$$

und es muss der Eine Theil puv^2 der Faktoren der rechten Seite auf $x+y$ und der andere Theil quw^2 auf $x-y$ kommen. Demnach hat man

(9) $$x + y = puv^2$$

(10) $$x - y = quw^2$$

und hieraus folgt als Auflösung der gegebenen Gl. (7)

(11) $$x = \frac{u(pv^2+qw^2)}{2}, \quad y = \frac{u(pv^2+qw^2)}{2}, \quad z = uvw$$

Es ist stets leicht dafür zu sorgen, dass ausser z auch x und y ganze Zahlen werden. Nachdem man nämlich für p, q irgend zwei Faktoren, in welche sich c zerlegen lässt, und für v, w zwei ganz willkürliche Zahlen substituirt hat, braucht man, wenn pv^2+qw^2 oder pv^2-qw^2 nicht durch 2 theilbar sind, nur für u irgend eine paare Zahl zu nehmen.

Beispiel. $x^2 - y^2 = 12z^2$ oder $x^2 = y^2 + 12z^2$
Die Zahl $c = 12$ kann auf irgend Eine der folgenden Arten in zwei Faktoren p, q zerlegt werden.

$p =$	1	2	3	4	6	12	-1	-2	-3	-4	-6	-12
$q =$	12	6	4	3	2	1	-12	-6	-4	-3	-2	-1

Nimmt man einmal $p = 3$, $q = 4$; so kommt

$$x = \frac{u(3v^2+4w^2)}{2}, \quad y = \frac{u(3v^2-4w^2)}{2}, \quad z = uvw.$$

Hierin kann man entweder für v paare und für u beliebige oder für v unpaare und für u paare Werthe setzen.

So hat man z. B. für $v=1$, $w=1$, $u=2$

$$x=7, \qquad y=-1, \qquad z=2$$

III. Es sei nun eine Gleichung von der Form

$$(12) \qquad \alpha^2x^2-\beta^2y^2=cz^2$$

oder auch

$$\alpha^2x^2=\beta^2y^2+cz^2$$

gegeben, worin die Koeffizienten α^2 und β^2 vollkommene Quadrate sind, c aber beliebig positiv oder negativ sein kann. Setzt man hier, wie früher $c=pq$, $z=uvw$; so hat man

$$(\alpha x+\beta y)(\alpha x-\beta y)=(puv^2)(quw^2)$$

also

$$(13) \qquad \alpha x+\beta y=puv^2$$

$$(14) \qquad \alpha x-\beta y=quw^2$$

Hieraus folgt die Auflösung

$$(15) \qquad x=\frac{u(pv^2+qw^2)}{2\alpha}, \qquad y=\frac{u(pv^2-qw^2)}{2\beta}, \qquad z=uvw$$

Um nicht bloss für z, sondern auch für x und y ganze Zahlen zu erhalten, kann man v und w beliebig annehmen, und wenn alsdann 2α nicht in pv^2+qw^2 oder 2β nicht in pv^2-qw^2 aufgeht, für u irgend einen Generalnenner der auf die kleinste Benennung gebrachten Brüche $\frac{pv^2+qw^2}{2\alpha}$ und $\frac{pv^2-qw^2}{2\beta}$ wählen.

Unter allen Umständen werden x, y, z ganze Zahlen, wenn man $u=2\alpha\beta u'$ also

$$(16) \qquad x=\beta u'(pv^2+qw^2), \qquad y=\alpha u'(pv^2-qw^2), \qquad z=2\alpha\beta u'vw$$

setzt. Obgleich hierin u', v, w völlig willkürlich bleiben; so ist doch nicht hierdurch, sondern durch (15) die allgemeine Auflösung der Gl. (12) dargestellt.

Nach der Natur der gegebenen Gleichung (12) leuchtet ein, dass jede der beiden Grössen α und β sowol positiv, wie auch negativ gedacht werden kann. Auf diese Zweideutigkeit braucht man dann kein Gewicht zu legen, wenn man sich vorbehält, jeden Werth von x, y, z sowol positiv wie negativ zu nehmen.

Es ist klar, dass die sub I. und II. behandelten Gleichungen nur spezielle Fälle der gegenwärtigen sind, und dass alle Gleichungen von dieser Form stets in ganzen Zahlen auflösbar sind.

Beispiel. $\qquad 4x^2-9y^2=-7z^2$ oder

$$2^2x^2-3^2y^2=-7z^2$$

Hier hat man wegen $c = -7$, $\begin{Bmatrix} p = & 1 & -7 \\ q = & -7 & 1 \end{Bmatrix}$. Nimmt man einmal $p = 1$, $q = -7$; so kommt

$$x = \frac{u(v^2 - 7w^2)}{4}, \quad y = \frac{u(v^2 + 7w^2)}{6}, \quad z = uvw$$

Setzt man $v = 1$, $w = 1$; so ergibt sich

$$x = -\frac{3u}{2}, \quad y = \frac{4u}{3}, \quad z = u$$

und es ist klar, dass jetzt für u irgend ein Generalnenner der Brüche $\frac{3}{2}$ und $\frac{4}{3}$, also irgend ein Vielfaches von 6 gesetzt werden muss. Für $u = 6$ würde man haben

$$x = -9, \quad y = 8, \quad z = 6$$

§. 161. ***Auflösung der Gleichung:***

(1) $$x^2 - by^2 = cz^2 \quad \text{oder} \quad x^2 = by^2 + cz^2$$

I. Wenn in dieser Gleichung b oder c ein vollkommenes Quadrat (mithin auch entschieden positiv) wäre; so würde dieselbe nach dem vorhergehenden Paragraphen, Satz III., sofort aufzulösen sein. Ist Dies jedoch nicht der Fall, und sind die Koeffizienten b und c entweder beide positiv oder der Eine positiv und der andere negativ (indem der Fall, wo beide negativ wären, also nur $x = 0$, $y = 0$, $z = 0$ sein könnte, ausgeschlossen bleibt); so schicken wir der weiteren Behandlung dieser Gleichung folgende Betrachtung voran.

Die aus der Entwickelung des Ausdruckes

(2) $$K = \frac{\sqrt{D} + P_0}{Q_0}$$

in einen Kettenbruch sich ergebenden Grössen liefern nach §. 68, Gl. 4, folgende bekannte Beziehungen

(3) $$(Q_0 M_{m+n} - P_0 N_{m+n})^2 - D N_{m+n}^2 = (-1)^0 Q_0 (-1)^{m+n+1} Q_{m+n+1}$$

Hierin sind die Grössen M_{m+n}, N_{m+n} Zähler und Nenner des Kettenbruches

(4) $$K_{m+n} = \frac{M_{m+n}}{N_{m+n}} = [a_0, a_1, a_2 \ldots a_m, a_{m+1} \ldots a_{m+n}]$$

Die durch M, N bezeichneten Grössen von den Zeigern m, $m-1$, $m-2$ erhält man, indem man den vorstehenden Kettenbruch resp. mit dem Quotienten a_m, a_{m-1}, a_{m-2} schliesst.

Setzt man, wie in §. 124, den reduzirten Kettenbruch

(5) $$\mathfrak{K}_n = \frac{\mathfrak{M}_n}{\mathfrak{N}_n} = [a_m, a_{m+1} \ldots a_{m+n}]$$

so erhält man, indem man die Gl. (5) in §. 124 mit Q_m multiplizirt und dann $Q_m Q_{m-1} = D - P_m^2$ substituirt, folgende der vorstehenden Gl. (3) ähnliche Formel.

(6) $(Q_m \mathfrak{M}_n - P_m \mathfrak{N}_n)^2 - D\mathfrak{N}_n^2 = (-1)^m Q_m (-1)^{m+n+1} Q_{m+n+1}$

Zwischen den Grössen M_{m+n}, N_{m+n} und $\mathfrak{M}_n$, $\mathfrak{N}_n$ bestehen nach §. 124, Gl. (9) bis (12) folgende Beziehungen

$$(7) \quad \begin{cases} M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n \\ N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n \end{cases}$$

$$(8) \quad \begin{cases} \mathfrak{M}_n = (-1)^m (N_{m-2}M_{m+n} - M_{m-2}N_{m+n}) \\ \mathfrak{N}_n = (-1)^m (M_{m-1}N_{m+n} - N_{m-1}M_{m+n}) \end{cases}$$

Denken wir uns, in den vorstehenden Formeln sei $(-1)^{m+n+1} Q_{m+n+1}$ ein vollkommenes Quadrat (also auch positiv), wogegen D und Q_0 beliebige positive oder negative Werthe haben mögen; so ist die Gl. (3) der Vertreter der gegebenen Gleichung (1). Hierin sei y die mit dem numerisch kleineren Koeffizienten behaftete der beiden Unbekannten y, z, also der numerische Werth von $b \leqq a$. Assimiliren wir nun die gegebene Gleichung in der Form

$$(9) \qquad x^2 - by^2 = cz^2$$

der Gl. (3); so haben wir

$$(10) \qquad D = b, \qquad Q_0 = c$$

$$(11) \quad x = Q_0 M_{m+n} - P_0 N_{m+n}, \; y = N_{m+n}, \; z = \sqrt{(-1)^{m+n+1} Q_{m+n+1}}$$

Zu den in Gl. (10) angegebenen Werthen von D und Q_0 ermitteln wir nun nach bekannten Regeln die Werthe von P_0, welche den verschiedenen Reihen der durch $Q_0 = c$ theilbaren Zahlen von der Form $D - P_0^2 = b - P_0^2$ entsprechen. Für jeden dieser Werthe von P_0 entwickeln wir den Ausdruck

$$(12) \qquad K = \frac{\sqrt{D} + P_0}{Q_0} = \frac{\sqrt{b} + P_0}{c}$$

in einen Kettenbruch.

Gibt es überhaupt keinen solchen Werth von P_0, also keine durch c theilbare Zahl von der Form $b - P_0^2$; so gibt es offenbar auch keine durch c theilbare Zahl von der Form $x^2 - by^2$ mit relativ primen Werthen für x und y, was unmittelbar aus dem fünften Abschnitte erhellet, also keine Auflösungen der gegebenen Gleichung mit relativ primen Werthen für x und y. Was jedoch die Auflösungen betrifft, in welchen x und y ein gemeinschaftliches Maass besitzen; so setzen offenbar diejenigen, welche irgend ein Maass u auch mit z gemein haben, das Vorhandensein der Auflösungen $\frac{x}{u}$, $\frac{y}{u}$, $\frac{z}{u}$ voraus, in welchen nicht alle drei Unbekannten ein

gemeinschaftliches Maass haben. Soll es aber Werthe von x, y geben, welche unter einander, nicht aber mit z ein gemeinschaftliches Maass besitzen; so muss nothwendig der Koeffizient c einen *quadratischen Faktor* besitzen. Hat also c keinen quadratischen Faktor; so sind auch Auflösungen der letzteren Art nicht möglich. Ist aber in c ein Quadrat als Faktor enthalten; so hat man dasselbe nach der später sub VII. mitzutheilenden Vorschrift zu berücksichtigen.

Nachdem man nun die Grösse K aus (12) in einen Kettenbruch mit grössten Subquotienten entwickelt hat, welcher, da nach der Voraussetzung $D = b$ kein Quadrat ist, jedenfalls *periodisch* sein wird; so kann man für jeden beliebigen Zeiger m die Gl. (6) bilden, welche durch Transposition in folgende Form übergeht,

$$(13) \quad (Q_m\mathfrak{M}_n - P_m\mathfrak{N}_n)^2 - (-1)^m Q_m (-1)^{m+n+1} Q_{m+n+1} = D\mathfrak{N}_n^2$$

Bei einem Übergange von der Gl. (3) zu der Gl. (13), welcher im Laufe der späteren Rechnung noch mehrmals vorkommen kann, werden wir die neu auftretenden Grössen immer mit denselben Buchstaben wie in Gl. (9), jedoch mit Einem Akzente mehr belegen, selbst wenn diese oder jede öfter akzentuirte Grösse genau den Werth einer schon früher vorgekommenen Grösse besässe. Demnach schreiben wir statt Gl. (13) als *erste transformirte Gleichung* kurz

$$(14) \quad x'^2 - b'y'^2 = c'z'^2$$

Hierin ist unter Berücksichtigung der Gleichungen (10), (11)

$$(15) \quad D' = b' = (-1)^m Q_m, \qquad Q_0' = c' = D = b$$

$$(16) \quad x' = Q_m\mathfrak{M}_n - P_m\mathfrak{N}_n, \quad y' = \sqrt{(-1)^{m+n+1}Q_{m+n+1}} = z, \quad z' = \mathfrak{N}_n$$

II. *Gibt es nun in der Entwickelung von K unter den Grössen $(-1)^m Q_m$ ein vollkommenes Quadrat;* so nehme man dasselbe für b'. Die Gl. (14) kann alsdann genau nach §. 160, III. für x', y', z' aufgelös't werden. Die hierfür gefundenen allgemeinen Ausdrücke führen dann vermöge der vorstehenden Beziehungen durch rückwärts gerichtete Substitutionen zu allgemeinen Werthen für x, y, z, welche die Auflösung der gegebenen Gl. (1) bilden. Man hat nämlich zu beachten, dass nach der dritten der Gleichungen (16) durch den Werth von z' der Werth von $\mathfrak{N}_n$, und demnach vermöge der ersten jener Gleichungen durch x' und z' auch der Werth

$$(17) \quad \mathfrak{M}_n = \frac{x' + P_m z'}{Q_m}$$

bestimmt ist. Da ferner P_m, Q_m, M_{m-1}, N_{m-1}, M_{m-2}, N_{m-2} die aus der Entwickelung von K resp. für die Zeiger m, $m-1$, $m-2$ zu entnehmenden Grössen sind; so führt Dies vermöge

der Formeln (7) zu Ausdrücken für M_{m+n}, N_{m+n}. Substituirt man die letzteren in die ersten beiden der Gleichungen (11); so erhält man die allgemeinen Ausdrücke für x und y. Was den Werth von z aus der dritten der Gleichungen (11) anlangt; so ist es nicht nöthig, wegen der Beziehung dieser Unbekannten zu der Grösse Q_{m+n+1} noch weitere Untersuchungen anzustellen, da man nach der zweiten der Gleichungen (16) einfach $z = y'$ hat.

Man hat also den durch folgende Gruppe von Gleichungen dargestellten einfachen Rücklauf von Substitutionen:

$$(G) \begin{cases} \mathfrak{M}_n = \dfrac{x' + P_m z'}{Q_m}, & \mathfrak{N}_n = z' \\ M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n, & N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n \\ x = Q_0 M_{m+n} - P_0 N_{m+n}, \quad y = N_{m+n}, \quad z = y' \end{cases}$$

In dieser Gruppe von Gleichungen haben die Grössen x', y', z' die aus der Auflösung der transformirten Gleichung (4) hervorgehenden Werthe.

III. **Gibt es aber in der obigen Entwickelung** von K **unter den Grössen** $(-1)^m Q_m$ **kein Quadrat**; so werden doch in der **Periode** dieser Grössen (wenn D positiv ist, nach §. 65, und wenn D negativ ist, nach §. 95) Werthe vorkommen, welche, numerisch genommen, **kleiner** als die Determinante $D = b$, aber > 0 sind, gleichviel, ob dieselben das positive oder negative Zeichen haben, insofern nicht etwa die Determinante $D = -1$ sein sollte, in welchem Falle man bei Ausschluss des quadratischen Werthes $(-1)^m Q_m = 1$ den Werth $(-1)^m Q_m = -1$ zu gewärtigen hat.

Von den letzteren Werthen wähle man irgend Einen für $(-1)^m Q_m = b'$. Behuf thunlichster Abkürzung der Rechnung wird man ohne Frage entweder das positive oder das negative **Minimum** der in der Periode von $(-1)^m Q_m$ erscheinenden Grössen nehmen. Ist das positive Minimum numerisch kleiner, als das negative; so verdient das erstere vor dem letzteren entschieden den Vorzug, ja oftmals auch selbst dann, wenn es grösser sein sollte, als das letztere.

Jetzt behandelt man die Gl. (14) behuf deren Auflösung genau ebenso, wie es vorstehend mit der Gl. (9) geschehen ist, indem man alle jetzt auftretenden Grössen mit denselben Buchstaben, wie früher, jedoch mit einem Akzente bezeichnet. Demnach treten jetzt an die Stelle der Grössen m, P, Q, M, N, $\mathfrak{M}$, $\mathfrak{N}$ etc. die Grössen m', P', Q', M', N', $\mathfrak{M}'$, $\mathfrak{N}'$ etc., welche eine ähnliche Bedeutung wie die früheren haben und demnach auch in einem durch die früheren Formeln angegebenen Zusammenhange stehen.

Zuvörderst entwickelt man also die Grösse

$$(18) \qquad K' = \frac{\sqrt{D'} + P'_0}{Q'_0} = \frac{\sqrt{b'} + P'_0}{c'}$$

in einen Kettenbruch mit grössten Subquotienten, indem man zur Bestimmung von P'_0 die Reihen der durch c' theilbaren Zahlen von der Form $b' - P'^2_0$ aufsucht, und nach und nach für P'_0 jeden der dafür sich ergebenden verschiedenen Werthe in den Ausdruck von K' treten lässt.

Für jeden beliebigen Zeiger m' aus dieser Entwickelung kann man nach Analogie der Gl. (13) die neue Gleichung

$$(19) \quad (Q'_{m'}\mathfrak{M}'_{n'} - P'_{m'}\mathfrak{N}'_{n'})^2 - (-1)^{m'}Q'_{m'}(-1)^{m'+n'+1}Q'_{m'+n'+1} = D'\mathfrak{N}'^2_{n'}$$

oder die zweite transformirte Gleichung

$$(20) \qquad x''^2 - b''y''^2 = c''z''^2$$

bilden, indem man nach Analogie der Gleichungen (15), (16)

$$(21) \quad D'' = b'' = (-1)^{m'}Q'_{m'}, \qquad Q''_0 = c'' = D' = b' = (-1)^m Q_m$$

$$(22) \quad x'' = Q'_{m'}\mathfrak{M}'_{n'} - P'_{m'}\mathfrak{N}'_{n'}, \quad y'' = \sqrt{(-1)^{m'+n'+1}Q'_{m'+n'+1}} = z', \quad z'' = \mathfrak{N}'_{n'}$$

setzt, woraus ähnlich wie in Gl. (17) auch

$$(23) \qquad \mathfrak{M}'_{n'} = \frac{z'' + P'_{m'}x''}{Q'_{m'}}$$

folgt.

IV. Jetzt sieht man nach, ob unter den Grössen $(-1)^{m'}Q'_{m'} = b''$ ein vollkommenes (also auch positives) Quadrat vorkommt. Ist Dies der Fall; so kann Gl. (20) nach §. 160, III. aufgelös't werden, und eine rückgängige Substitution der hierdurch für x'', y'', z'' gefundenen Ausdrücke, welche durch eine der obigen Gruppe (G) ganz gleiche Gruppe (G') zu bewirken ist, liefert zunächst Ausdrücke für x', y', z', und hierdurch gelangt man durch die Gruppe (G') weiter zu den gesuchten Ausdrücken für x, y, z, welche die Auflösung der gegebenen Gl. (1) bilden.

V. Findet sich aber unter den Grössen $(-1)^{m'}Q'_{m'} = b''$ kein vollkommenes Quadrat; so nimmt man wieder aus der Periode derselben das positive oder negative Minimum, welches jedenfalls kleiner, als die Determinante $D' = b'$ sein wird, und verfährt mit der Gl. (20), wie es für die Gl. (9) und (14) vorgeschrieben war. Dies wird die dritte transformirte Gleichung von der Form

$$(24) \qquad x'''^2 - b'''y'''^2 = c'''z'''^2$$

erzeugen, u. s. f.

Da bei diesen Verwandlungen die erste Determinante $D = b$ numerisch $< c$ ist und alle Determinanten D, D', D'' ... oder

$b, b', b'' \ldots$ oder $b, (-1)^m Q_m, (-1)^{m'} Q'_{m'} \ldots$ eine abnehmende Reihe bilden; so muss man durch dieses Verfahren unter den eben genannten Grössen, wennicht früher auf ein Quadrat > 1, endlich entweder auf das Quadrat 1 oder aber auf den schon vorhin angemerkten Fall stossen, wo die Determinante den Werth -1 und auch die nächste folgende Grösse den Werth -1 hat.

Im letzteren Falle gelangt man zu einer Gleichung von der Form $X^2 + Y^2 = -Z^2$ oder $X^2 + Y^2 + Z^2 = 0$, welche offenbar alle anderen Auflösungen, ausser $x = 0$, $y = 0$, $z = 0$ als unmögliche erscheinen lässt. Dieser Fall wird sich ereignen, wenn in der gegebenen Gl. (1) die beiden Koeffizienten b und c negativ sind.

In jedem anderen Falle wird man die Auflösung der Schlussgleichung nach §. 160, III. bewirken und durch rückgängige Substitutionen zu der Auflösung x, y, z der gegebenen Gleichung gelangen können.

Bei der Auflösung der Schlussgleichung muss darauf geachtet werden, dass dieselbe in aller Vollständigkeit nach §. 160, III. erfolgt. Es ist also die Vielfachheit der Werthe der Faktoren p, q sowie die Willkürlichkeit der Zeichen der Grössen u, v, w oder auch der in der Schlussgleichung vorkommenden Unbekannten gehörig zu berücksichtigen.

VI. Es würde nicht schwer sein, die allgemeinen Formeln hier niederzuschreiben, welche die Werthe von x, y, z, ausgedrückt durch die Auflösung der Schlussgleichung, darstellen. Es ist jedoch viel einfacher, in jedem speziellen Falle die betreffenden Substitutionen auszuführen. Zu diesem Ende ist es sogar zweckmässig, wenn z. B. (24) die Schlussgleichung wäre, nicht sofort die nach §. 160, III. für x''', y''', z''' sich ergebenden allgemeinen Ausdrücke in u, v, w, p, q zu bilden und durch alle Substitutionsformeln bis zu den Werthen von x, y, z hinaufzuführen, sondern in diese Formeln zuvörderst die einfachen Zeichen x''', y''', z''' zu substituiren, also zuvörderst x, y, z durch x''', y''', z''' auszudrücken, und dann erst für x''', y''', z''' ihre allgemeinen Ausdrücke in u, v, w, p, q an die Stelle zu setzen.

Was die allgemeine Form der Ausdrücke anlangt, in welcher sich schliesslich die Werthe von x, y, z darstellen werden; so ist aus dem Wesen der vorzunehmenden Substitutionen und aus der Form der Auflösung der Schlussgleichung nach §. 160, III. leicht zu erkennen, dass man erhalten wird

$$(25)\quad \left\{ \begin{aligned} x &= \frac{u(Av^2 + Bw^2 + Cvw)}{E} \\ y &= \frac{u(A_1v^2 + B_1w^2 + C_1vw)}{E_1} \\ z &= \frac{u(A_2v^2 + B_2w^2 + C_2vw)}{E_2} \end{aligned} \right.$$

Es kann also jederzeit leicht dafür gesorgt werden, dass x, y, z ganze Zahlen werden. Man braucht zu diesem Ende nur für v und w beliebige ganze Zahlen zu setzen, und dann für u irgend einen Generalnenner der auf die kürzeste Benennung gebrachten Brüche, in welche u multiplizirt ist, zu substituiren.

Jedenfalls erzeugen sich also ganze Zahlen, wenn man für u irgend ein Vielfaches von EE_1E_2 nimmt.

Man erkennt ferner, dass in die Nenner E, E_1, E_2 keine anderen Zahlen, als 2, Q_m, $Q'_{m'}$, $Q''_{m''}$ ... eintreten, sodass jeder Werth von u, welcher ein Vielfaches von $2Q_mQ'_{m'}Q''_{m''}$ ... ist, in allen Fällen für x, y, z ganze Zahlen ergibt.

VII. Jetzt bleibt noch aus dem schon früher angeführten Grunde zu untersuchen, ob nicht etwa die Grössen $Q_0 = c$, $Q'_0 = c'$, $Q''_0 = c''$ quadratische Faktoren enthalten. Überall, wo dieser Umstand bei irgend Einer der gegebenen oder transformirten Gleichungen (9), (14), (20)..., welche nicht die Schlussgleichung ist, eintritt, sind nacheinander alle einzelnen verschiedenen quadratischen Faktoren von einer solchen Grösse abzusondern, und für jeden solchen quadratischen Faktor nach folgender Regel zu verfahren.

Angenommen, es sei in der Gl. (9) $Q_0 = c = \gamma^2 c_1$. Alsdann ist diese Gleichung ausser in der obigen Weise, welche den Zweck hat, die relativ primen Werthe von x und y herauszustellen, noch auf die etwaigen Auflösungen zu prüfen, in welchen selbst die kleinsten Werthe von x und y das gemeinschaftliche Maass γ besitzen. Zu diesem Ende stösst man im Sinne der ähnlichen Rechnung im fünften Abschnitte den quadratischen Faktor γ^2 aus der rechten Seite der Gl. (9) heraus, und lös't die Gleichung

$$(26)\qquad x_1^2 - by_1^2 = c_1 z_1^2$$

nach der obigen Methode auf. Nachdem Dies geschehen, hat man als Auflösungen der gegebenen Gleichung

$$(27)\qquad x = \gamma x_1, \qquad y = \gamma y_1, \qquad z = z_1$$

Diese Berücksichtigung der quadratischen Faktoren ist weder eine Sache des Beliebens, welche auch unterlassen werden dürfte, noch ein Ersatz für die Ausführung der früher beschriebenen Rechnung.

Die Natur der mit und ohne Berücksichtigung jener quadratischen Faktoren sich ergebenden Auflösungen ist in Hinsicht auf gemeinschaftliche Theilbarkeit verschieden, und wie bei den Gleichungen mit 2 Unbekannten im fünften Abschnitte; so kann es sich auch hier ereignen, dass von den bezeichneten beiden Arten von Auflösungen bald beide, bald keine, bald aber nur die Eine oder die andere möglich sind.

Es scheint, als ob man die Rolle, welche die quadratischen Faktoren der Koeffizienten in den unbestimmten Gleichungen vom zweiten Grade spielen, bisweilen verkannt und die Vollständigkeit der Auflösungen durch das unbedingte Hinauswerfen jener Faktoren beeinträchtigt habe.

Die vorstehende Auflösungsmethode hat eine gewisse Verwandtschaft mit der von Lagrange in seinen Zusätzen zu Eulers Algebra, Kap. V, vorgetragenen und später von Legendre in der *Théorie des nombres*, *§. III.*, reproduzirten Methode, jedoch nur in dem Grundgedanken der Transformation mit immer kleiner werdenden Koeffizienten, nicht in der Ausführung dieses Prinzips. Namentlich gewährt unsere Methode, da sie die Anzahl der Transformationen und der hiermit verbundenen umständlichen Nebenrechnungen auf ein Minimum beschränkt, den Vortheil der grösseren Kürze in einem sehr erheblichen Grade, wie wir in §. 166 an einem auch von Lagrange berechneten Beispiele zeigen wollen.

VIII. Es ist noch von Interesse, zu bemerken, dass die obige Rechnung ein Mittel an die Hand gibt, eine der Kettenbruchsentwickelung $K=\frac{\sqrt{D}+P_0}{Q_0}$ angehörige Grösse $(-1)^{m+n+1}Q_{m+n+1}$ zu bestimmen, welche ein vollkommenes Quadrat ist, wenn es überhaupt deren gibt. Zu diesem Ende bildet man die Gleichung $x^2-Dy^2=Q_0z^2$, welche die Stelle von Gl. (3) vertritt und auflösbar sein muss. Schliesslich hat man wegen Gl. (11)

$$N_{m+n}=y,\quad M_{m+n}=\frac{x+P_0y}{Q_0}\quad \text{also}\quad \frac{M_{m+n}}{N_{m+n}}=\frac{x+P_0y}{Q_0y}$$

Verwandelt man also irgend Einen der durch x und y bedingten Werthe des Bruches $\frac{M_{m+n}}{N_{m+n}}$ in einen Kettenbruch $[a_0, a_1 \ldots a_{m+n}]$; so liefert die Einführung der Quotienten dieses Kettenbruches in die Entwickelung von K bei dem Zeiger $m+n+1$ eine Grösse $(-1)^{m+n+1}Q_{m+n+1}$, welche ein vollständiges Quadrat ist. Wenn sich für M_{m+n} und N_{m+n} relativ prime Werthe ergeben, ist offenbar $(-1)^{m+n+1}Q_{m+n+1}=z^2$. Haben aber M_{m+n} und N_{m+n} das grösste gemeinschaftliche Maass μ; so wird $(-1)^{m+n+1}Q_{m+n+1}=\left(\frac{z}{\mu}\right)^2$ sein.

§. 162. ***Anzahl der nach vorigem Paragraphen auszuführenden Transformationen.***

I. Es ist von Interesse, von vorn herein übersehen zu können, wie gross **höchstens** die Anzahl der vorzunehmenden Transformationen sein kann, welche man nach dem vorstehenden Paragraphen ausführen muss, um zu einer transformirten Gleichung zu gelangen, deren zweiter Koeffizient auf der linken Seite ein Quadrat ist. Unterscheiden wir hierbei zwei Fälle.

Der günstigste Fall ist im Allgemeinen der, wo alle Determinanten D, D', D'' ... positiv ausfallen. Alsdann ist jede folgende Determinante, wie $D' = (-1)^m Q_m$, welche das Minimum der periodischen Grössen Q aus der der vorhergehenden Determinante D angehörigen Entwickelung darstellt, nach §. 65 kleiner als $\sqrt{D}$. Wenn sich also nicht schon früher ein Quadrat > 1 einstellt, wenn also die schlimmste Nothwendigkeit eintritt, soweit fortzurechnen, bis sich das Quadrat 1 herausstellt; so hat man folgende Reihe von Beziehungen.

$$D' < \sqrt{D} \text{ oder } \sqrt{b}, \qquad D'' < \sqrt{D'} \text{ oder } \sqrt[4]{b},$$
$$D''' < \sqrt{D''} \text{ oder } \sqrt[8]{b}, \quad D'''' < \sqrt{D'''} \text{ oder } \sqrt[16]{b} \text{ u. s. w.}$$

Die erste Determinante, welche der Entwickelung von K zu Grunde liegt, ist $D = b$. Erwägt man nun, dass wenn die Rechnung nicht schon früher ihr Ende erreicht, es darauf ankommt, dass die letzte Determinante $= 1$, also < 2 werde; so ergibt sich Folgendes.

Man braucht nur diese einzige erste Entwickelung zu machen, wenn $\sqrt{b} < 2$, also $b < 4$ ist.

Die zweite Determinante, welche der Entwickelung von K' zu Grunde liegt, ist $D' < \sqrt{b}$. Man braucht also höchstens zwei Entwickelungen zu machen, wenn $\sqrt{D'} < 2$ oder $\sqrt[4]{b} < 2$ oder $b < 16$ ist.

Ueberhaupt beträgt die Anzahl der Entwickelungen

wenn	$\sqrt{b} < 2$	oder	$b < 4$	ist,	höchstens	1
»	$\sqrt[4]{b} < 2$	»	$b < 16$	»	»	2
»	$\sqrt[8]{b} < 2$	»	$b < 256$	»	»	3
»	$\sqrt[16]{b} < 2$	»	$b < 65536$	»	»	4
			allgemein			
»	$\sqrt[2^n]{b} < 2$	»	$b < 2^{2^n}$	»	»	n

II. Der ungünstigste Fall ist der, wo unter den Determinanten auch negative Werthe vorkommen. Man erkennt jedoch, dass niemals zwei unmittelbar auf einander folgende Determinanten, z. B. nicht D und $D' = (-1)^m Q_m$, zugleich negativ sein können, weil Dies sofort zu der Gl. (14) führen würde, in welcher die linke Seite entschieden positiv und die rechte entschieden negativ wäre. Eine solche Gleichung entsteht, wenn in der gegebenen Gl. (1) die beiden Koeffizienten b und c negativ sind, ein Fall, welcher nur die Auflösung $x = 0$, $y = 0$, $z = 0$ zulässt, und von vorn herein ausgeschlossen sein soll. Es müssen also im gegenwärtigen Falle wenigstens positive Determinanten mit negativen abwechseln. Die Verkleinerung der nächstfolgenden Determinante D', wenn die vorhergehende D positiv ist, haben wir schon angezeigt; es würde nämlich numerisch $D' < \sqrt{D}$ sein, wobei D' negativ sein kann. Wenn jedoch die vorhergehende Determinante D negativ ist, hat man nach §. 95 für das periodische Minimum der Grössen $(-1)^m Q_m$ (welche sämmtlich einerlei und zwar hier das positive Zeichen besitzen werden) indem man mit D den numerischen Werth dieser Determinante bezeichnet,

$$(-1)^m Q_m = D' \leqq \frac{D+1}{2}.$$

Hieraus ergibt sich, dass wenn b positiv ist, man höchstens 1, 2, 3, 4, 5... Entwickelungen zu machen hat, jenachdem resp. $\sqrt{b}$, $\frac{1}{2}(1+\sqrt{b})$, $\sqrt{\frac{1}{2}(1+\sqrt{b})}$, $\frac{1}{2}\left(1+\sqrt{\frac{1}{2}(1+\sqrt{b})}\right)$, $\sqrt{\frac{1}{2}\left(1+\sqrt{\frac{1}{2}(1+\sqrt{b})}\right)} \ldots < 2$ oder jenachdem b resp. < 4, 9, 49, 289, 9409... ist. Wäre dagegen der fragliche Koeffizient negativ $= -b$; so hätte man höchstens 1, 2, 3, 4, 5, 6... Entwickelungen zu machen, jenachdem resp. $\frac{1}{2}(1+b)$, $\sqrt{\frac{1}{2}(1+b)}$, $\frac{1}{2}\left(1+\sqrt{\frac{1}{2}(1+b)}\right)$, $\sqrt{\frac{1}{2}\left(1+\sqrt{\frac{1}{2}(1+b)}\right)}$,

$$\frac{1}{2}\left(1+\sqrt{\frac{1}{2}\left(1+\sqrt{\frac{1}{2}(1+b)}\right)}\right),$$

$\sqrt{\frac{1}{2}\left(1+\sqrt{\frac{1}{2}\left(1+\sqrt{\frac{1}{2}(1+b)}\right)}\right)} \ldots < 2$ oder jenachdem b resp. < 3, 7, 17, 97, 577, 18817 ist.

Entwickelte man die Kettenbrüche mit negativer Deter-

minante nach §. 98; so wird das Minimum von $(-1)^m Q^m = D' \leqq \sqrt{\frac{4D}{3}}$, und der Schluss der Rechnung wird noch rascher erreicht. Man hat alsdann, wenn b positiv ist, höchstens 1, 2, 3, 4, 5... Entwickelungen zu machen, jenachdem resp.

$$\sqrt{b},\ \sqrt{\frac{4}{3}\sqrt{b}},\ \sqrt[4]{\frac{4}{3}\sqrt{b}},\ \sqrt{\frac{4}{3}\sqrt[4]{\frac{4}{3}\sqrt{b}}},\ \sqrt[4]{\frac{4}{3}\sqrt[4]{\frac{4}{3}\sqrt{b}}}\ldots < 2$$

oder jenachdem b resp. $< 4, 9, 144, 3691, 30233088\ldots$ ist. Wäre dagegen der fragliche Koeffizient negativ $= -b$; so hätte man höchstens 1, 2, 3, 4... Entwickelungen zu machen, jenachdem resp. $\sqrt{\frac{4}{3}b},\ \sqrt[4]{\frac{4}{3}b},\ \sqrt{\frac{4}{3}\sqrt[4]{\frac{4}{3}b}},\ \sqrt[4]{\frac{4}{3}\sqrt[4]{\frac{4}{3}b}}\ldots < 2$ oder jenachdem b resp. $< 3, 12, 61, 15552\ldots$ ist.

III. Hieraus ersieht man, dass man sich durch das obige Verfahren selbst bei grossen Zahlen sehr rasch dem Ende der Rechnung nähert. Zu diesem Zwecke muss auch noch darauf aufmerksam gemacht werden, dass es wegen der bei positiven Determinanten in der Regel rascheren Verminderung der Zahlen oftmals vorzuziehen ist, aus der Periode der Grössen $(-1)^m Q_m$ nicht das absolute Minimum zu nehmen, wenn dasselbe negativ ist, sondern das positive Minimum, welches nach §. 65 doch immer $< 2\sqrt{D}$ sein wird.

In dieser Rücksicht kann man auch gleich von vorn herein, wenn in der gegebenen Gleichung der Koeffizient b negativ sein sollte, weil alsdann jedenfalls der andere Koeffizient c positiv sein muss, das Glied cz^2 transponiren, also statt der Gl. $x^2 - by^2 = cz^2$ die Gleichung

$$x^2 - cz^2 = by^2$$

der obigen Behandlung unterwerfen.

§. 163. Kennzeichen der Lösbarkeit der Gleichung $x^2 = by^2 + cz^2$.

I. Nach der Natur der Gleichung von der Form $ax^2 = by^2 + cz^2$ kann man jede Auflösung x, y, z derselben mit jeder beliebigen ganzen oder gebrochenen Zahl multipliziren. Demnach sind Auflösungen in ganzen und in rationalen Zahlen gleichzeitig entweder beide möglich oder beide unmöglich.

Ferner ist klar, dass wenn die Koeffizienten a, b, c theilweise oder sämmtlich quadratische Faktoren enthielten, wenn also $a_1\alpha^2 x^2 = b_1\beta^2 y^2 + c_1\gamma^2 z^2$ gegeben wäre, diese Gleichung

32*

und die durch Absonderung der quadratischen Faktoren entstehende Gleichung $a_1X^2 = b_1Y^2 + c_1Z^2$ gleichzeitig entweder beide möglich oder beide unmöglich sind.

Wenn es also bloss auf die Prüfung der Lösbarkeit oder Unlösbarkeit einer Gleichung dieser Art ankommt, kann man sich auf die Betrachtung derjenigen Gleichung beschränken, welche entsteht, wenn die Koeffizienten von ihren etwaigen quadratischen Faktoren befreiet werden. Wir setzen also voraus, dass in der jetzt zu untersuchenden Gleichung $x^2 = by^2 + cz^2$ weder b, noch c einen quadratischen Faktor enthalte.

Auch nehmen wir an, dass nicht gleichzeitig b und c negativ seien; da sonst nur die Auflösung $x = 0$, $y = 0$, $z = 0$ möglich wäre.

Schon im vorstehenden Paragraphen ist bemerkt, dass man die nach §. 161 auszuführende Entwickelung sowol mit der Gleichung $x^2 - by^2 = cz^2$, als auch mit der Gleichung $x^2 - cz^2 = by^2$ beginnen kann. Damit sich dieser Entwickelung nicht gleich von vorn herein eine Unmöglichkeit entgegenstelle, muss es nach §. 161, I. sowol Zahlen von der Form $b - p^2$, welche durch c theilbar sind, als auch Zahlen von der Form $c - p^2$, welche durch b theilbar sind, geben.

Es muss also b ein quadratischer Rest nach c und auch c ein quadratischer Rest nach b, d. h. in kurzer Formelnsprache, es muss bRc und cRb sein.

Fände das Eine oder das Andere nicht statt; so wäre die gegebene Gleichung unmöglich. Ist aber Beides erfüllt; so ist man zu dem Schlusse, dass ausser $x = y = z = 0$ noch andere Auflösungen vorhanden seien, nur dann berechtigt, wenn die beiden Koeffizienten b und c relativ prim sind. Wären dieselben nicht relativ prim, besässen sie vielmehr das grösste gemeinschaftliche Maass a; so bedarf es noch der Erfüllung einer dritten Bedingung. Diese drei Bedingungen lassen sich, wenn man die gegebene Gleichung statt in Einer der obigen Formen in Einer der nachstehenden Formen

(1) $$x^2 = aby^2 + acz^2$$

(2) $x^2 - aby^2 = acz^2$ (3) $x^2 - acz^2 = aby^2$

aufstellt, nach Legendres *Théorie des nombres* dahin aussprechen, dass es Zahlen von der Form $ab - x^2$, $ac - x^2$, $bc + x^2$ geben müsse, welche resp. durch c, b, a theilbar seien, dass also gleichzeitig

(4) $abRc$, $acRb$, $-bcRa$

sein müsse.

Die ersten beiden dieser drei Bedingungen sind mit den vorhin erwähnten beiden Bedingungen, welche nach der jetzt gewählten Form der gegebenen Gleichung

(5) $abRac$, $acRab$

sein würden, als gleichbedeutend anzusehen, indem diese zu jenen und jene zu diesen führen. Denn da nach der Voraussetzung die beiden Koeffizienten ab und ac keinen quadratischen Faktor besitzen; so sind je zwei der Zahlen a, b, c relativ prim, und demnach sind auch ab und c, sowie ac und b relativ prim. Bestehen aber unter solchen Umständen die ersten beiden der Formeln (4); so bestehen auch, da stets $abRa$ und $acRa$ ist, nach §. 150, X. die beiden Formeln (5). Dass umgekehrt, wenn die beiden Formeln (5) bestehen, auch die ersten beiden der Formeln (4) erfüllt sind, ist für sich klar.

Was die dritte der Bedingungen (4) betrifft, welche immer dann realisirt sein wird, wenn die beiden Koeffizienten der gegebenen Gleichung relativ prim sind, also $a=1$ ist, und deren Nothwendigkeit sich sofort ergibt, wenn man einmal die Gl. (1) mit ab multiplizirt und die dabei entstehenden quadratischen Faktoren ausstösst; so wollen wir, ehe wir zum Beweise der daran sich knüpfenden Thatsache schreiten, jene Bedingung so modifiziren, dass sie in eine bemerkenswerthe Beziehung zu den Grössen tritt, welche bei der Kettenbruchsentwickelung des schon in §. 161 betrachteten Ausdruckes K zur Erscheinung kommen.

II. Setzt man behuf der in §. 161 bezeichneten Kettenbruchsentwickelung nach Maassgabe der Gl. (2) jetzt $D=ab$, $Q_0=ac$, schreibt auch zur Abkürzung für die in der Entwickelung von $K=\frac{\sqrt{D}+P_0}{Q_0}$ auftretenden Grössen $(-1)^m Q_m$ das einfachere Symbol q_m; so kann man zwischen der gegebenen Gleichung (9) in §. 161, welche in dieser Kettenbruchsentwickelung dem Zeiger 0 entspricht, und der ersten transformirten Gleichung (14) in §. 161, welche dem Zeiger m entspricht, folgende, den Zeigern 0, 1, 2 ... m entsprechende ähnlich gebildete Gleichungen schreiben, wovon eine jede in doppelter Gestalt, wie die vorstehenden beiden Gleichungen (2), (3) notirt werden soll. Dies gibt zwei Gruppen (A) und (B), in deren einzelnen Gliedern der kürzeren Schreibweise wegen die Unbekannten immer mit demselben Zeichen belegt sind.

	(A)		(B)
(6)	$x^2-Dy^2=q_0z^2$	(7)	$x^2-q_0z^2=Dy^2$
(8)	$x^2-Dy^2=q_1z^2$	(9)	$x^2-q_1z^2=Dy^2$
(10)	$x^2-Dy^2=q_2z^2$	(11)	$x^2-q_2z^2=Dy^2$
	$\vdots$		$\vdots$
(12)	$\begin{cases} x^2-Dy^2=q_m z^2 \\ x'^2-q_0 z'^2=Dy'^2 \end{cases}$	(13)	$\begin{cases} x^2-q_m z^2=Dy^2 \\ x'^2-Dy'^2=q_0 z'^2 \end{cases}$

Die erste transformirte Gleichung (14) in §. 161 erscheint hier als Gl. (13).

Die beiden Bedingungen (5), welche auch die ersten beiden der Bedingungen (4) vertreten, sind jetzt DRq_0 und q_0RD. Berücksichtigt man jetzt die Grösse Q vom Zeiger -1, welche bekanntlich $Q_{-1} = \frac{D - P_0^2}{Q_0}$ ist; so kann man für die dritte der Gleichungen (4), wie sogleich gezeigt werden soll, auch die Bedingung $q_{-1}RD$ an die Stelle setzen. Dass ausserdem DRq_{-1} sein wird, sobald nach der ersten Bedingung DRq_0 ist, leuchtet von selbst ein, weil man $D - P_0^2 = Q_0Q_{-1} = -q_0q_{-1}$ hat. Es geschieht also nur der Symmetrie der Formeln wegen, dass wir den obigen drei Bedingungen, die Bedingung DRq_{-1} als vierte hinzufügen und demgemäss die Lösbarkeit der gegebenen Gleichung (1) von der Existenz der Formeln

(14) DRq_{-1} (15) $q_{-1}RD$

(16) DRq_0 (17) q_0RD

abhängig machen.

Ehe wir den Beweis antreten, dass diese Formeln wirklich die Kennzeichen der Lösbarkeit der gegebenen Gleichung darstellen, wollen wir zeigen, dass die Bedingung (15) die dritte der Bedingungen (4) vollständig vertritt und umgekehrt.

Zu diesem Ende hat man $q_{-1} = -Q_{-1} = -\frac{D - P_0^2}{Q_0}$ $= -\frac{ab - P_0^2}{ac}$, d. i. da hierin P_0 offenbar durch die mit keinem quadratischen Faktor behaftete Zahl a theilbar, also $\frac{P_0}{a} = p$ eine ganze Zahl sein muss, $q_{-1} = \frac{-b + ap^2}{c}$, und hieraus folgt $c^2q_{-1} = -bc + acp$.

Nimmt man nun die Formel (15) als gegeben an; so hat man auch $c^2q_{-1}RD$ d. i.

(18) $(-bc + acp^2)Rab$ folglich gleichzeitig

(19) $(-bc + acp^2)Ra$ und $(-bc + acp^2)Rb$ oder

(20) $-bcRa$ und acp^2Rb

Die erste dieser beiden Formeln stimmt mit der dritten der Formeln (4) überein, und die zweite ist durch die zweite der Formeln (4) realisirt.

Nimmt man dagegen umgekehrt die Formeln (4) als gegeben an; so sind zunächst die Formeln (20) erfüllt, demnach auch die Formel (19) und alsdann, da a und b relativ prim sind, die Formel (18) oder $c^2q_{-1}RD$. Hieraus aber folgt, weil

c und $D = ad$ relativ prim sind, dass auch $q_{-1}RD$, also die Formel (15) erfüllt sein müsse (§. 150, XII.).

III. Was nun den Beweis betrifft, dass die Bedingungen (14) bis (17), oder eigentlich die drei letzten derselben, zur Lösbarkeit der Gl. (1) nothwendig und hinreichend sind; so erhellet deren Nothwendigkeit schon aus ihrer Ableitung. Um aber zu zeigen, dass sie zu dem fraglichen Zwecke auch hinreichend sind, beweisen wir zunächst, dass wenn sie bestehen, auch für jeden späteren Zeiger m die analogen Formeln

(21) DRq_m (22) q_mRD

bestehen werden.

Die Formel (21) erhellet aus der Gleichung (7) des §. 61, wonach $D - P_m^2 = Q_{m-1}Q_m = -q_{m-1}q_m$, also DRq_m ist.

Um die Formel (22) nachzuweisen; so hat man nach Gl. (4) oder (15) in §. 68 sofort q_0q_mRD, also wegen (17) auch $q_0^2q_mRD$ d. i. $(ac)^2q_mRab$, mithin auch $(ac)^2q_mRb$, und da ac und b relativ prim sind, nach §. 150, XII. q_mRb.

Nach Gl. (16) in §. 68 hat man ferner $q_{-1}q_mRD$, also wegen (15) auch $q_{-1}^2q_mRD$, mithin, da $D = ab$ ist, $q_{-1}^2q_mRa$. Es ist aber die Grösse $q_{-1} = \frac{-b + ap^2}{c}$ offenbar zu a relativ prim, weil b zu a relativ prim ist. Demnach hat man nach §. 150, XII. auch q_mRa.

Wenn aber nach Vorstehendem q_mRa und q_mRb; so ist auch, da a und b relativ prim sind, q_mRab d. i. q_mRD, wodurch die Formel (22) nachgewiesen ist.

IV. Besässe die Grösse q_m einen quadratischen Faktor; so kann derselbe abgesondert und in den Gleichungen (12) und (13) mit dem Quadrate z^2 der Unbekannten vereinigt werden, wie es schon vorhin für den Fall vorgeschrieben war, dass D oder q_0 einen quadratischen Faktor besässe. Wir behaupten, dass nach Absonderung dieses quadratischen Faktors nicht bloss die Formeln (21) und (22) für den Zeiger m, sondern auch die um Einen Zeiger zurückstehenden Formeln (also die für den Zeiger $m - 1$, worin natürlich auch q_{m-1} seinen Werth ändern wird) Gültigkeit behalten werden.

Um Dies nachzuweisen, wollen wir zeigen, dass wenn die vier Formeln (14) bis (17) für den Fall bestehen, dass q_0 einen quadratischen Faktor besitzt, sie auch bestehen werden, wenn dieser Faktor von q_0 getrennt wird (wodurch auch q_{-1} seinen Werth ändert), wobei jedoch die frühere Voraussetzung bestehen bleibt, dass D keinen quadratischen Faktor enthalte.

Denn ist $q_0 = \alpha^2k_0$; so folgt aus (16) oder aus $DR\alpha^2k_0$ auch sofort DRk_0.

Da α nothwendig relativ prim zu D sein muss, weil sonst die Formel (16) nach §. 150, XI. eine Unmöglichkeit enthielte; so bedingt die Formel (17) oder $\alpha^2 k_0 RD$ nach §. 150, XII. auch die Beziehung $k_0 RD$.

Die jetzt an die Stelle von q_{-1} tretende Grösse k_{-1} ist $=\alpha^2 q_{-1}$, indem man dafür $D - P_0^2 = -q_0 q_{-1} = -k_0 k_{-1}$ hat. Aus der letzteren Formel ergibt sich ohne Weiteres DRk_{-1}.

Endlich erkennt man, dass aus (15) auch $\alpha^2 q_{-1} RD$, d. i. $k_{-1} RD$ folgt.

V. Nach dem Vorstehenden kann man also in die Formeln (16) und (17) für q_0 nach und nach alle Werthe q_{-1}, q_0, q_1, q_2... substituiren.

Sobald man auf diese Weise bis zur ersten transformirten Gleichung (3) gelangt ist, welche sich durch Transposition aus der Gleichung (12) der Gruppe (A) ergibt, ändert sich für die fernere Entwickelung nach §. 161 der Werth der Determinante D, indem man jetzt $D' = q_m$ und $q_0' = D$ hat, und auch durch Absonderung des etwa in q_m enthaltenen quadratischen Faktors dafür sorgen kann, dass weder D', noch q_0' einen quadratischen Faktor besitze. Wie sich nun früher aus der Gleichung (6) die Gleichungen der Gruppen (A) und (B) erzeugten, so muss es jetzt, wenn die gegebene Gleichung lösbar sein soll, möglich sein, aus der Gleichung (13) zwei Gruppen (A') und (B') zu erzeugen, welche ebenso wie die früheren Gleichungen geschrieben werden können, wenn man alle darin vorkommenden Buchstaben akzentuirt. Eine solche Entwickelung würde offenbar dann möglich sein, wenn die Formeln (14) bis (17) auch für die akzentuirten Grössen beständen, indem es dann zunächst Werthe für P_0' gäbe, wodurch $D' - P_0'^2$ durch Q_0' theilbar würde und $K' = \frac{\sqrt{D'} + P_0'}{Q_0'}$ in einen Kettenbruch entwickelt werden könnte. Bedingten ausserdem die Formeln (14) bis (17) auch für die neuen Gleichungen analoge Beziehungen; so würden diese Beziehungen nicht bloss für die zunächst entstehenden Gruppen (A'), (B') bis zur zweiten transformirten Gleichung, sondern auch für alle ferneren Gruppen Bestand behalten, also nothwendig zu einer Auflösung der gegebenen Gleichung führen.

Um zu zeigen, dass Dem wirklich so ist, wollen wir darthun, dass die Formeln (14) bis (17) auch dann noch bestehen, wenn man in der gegebenen Gleichung (6) die beiden Koeffizienten D und q_0 mit einander vertauscht, also die durch Transposition daraus gebildete Gleichung (7) dafür an die Stelle setzt, während Gl. (6) an die Stelle von (7) tritt. Nimmt man also $D' = q_0$ und $q_0' = D$; so ist zu zeigen, dass auch sei

(23) $D'Rq'_{-1}$ (24) $q'_{-1}RD'$

(25) $D'Rq_0'$ (26) $q_0'RD'$

Setzt man für D' und q_0' ihre Werthe; so zeigen sich die beiden Formeln (25) und (26) als identisch resp. mit (17) und (16).

Aus (25) folgt dann von selbst auch (23), indem es danach einen Werth P_0' geben muss, wofür $D' - P_0'^2$ durch Q_0' theilbar, also $D' - P_0'^2 = Q_0'Q_{-1}' = - q_0'q_{-1}'$ wird.

Was endlich die Formel (24) betrifft, worin $D' = q_0 = ac$ ist; so wird dieselbe, da a und c relativ prim sind, dann und auch nur dann bestehen, wenn gleichzeitig $q_{-1}'Ra$ und $q_{-1}'Rc$ oder auch, da b relativ prim zu a und zu c ist, wenn gleichzeitig $b^2q_{-1}'Ra$ und $b^2q_{-1}'Rc$ ist. Nun hat man aber $q_{-1}' = \frac{-D' + P_0'^2}{q_0'}$ oder da $D' = q_0 = ac$, $q_0' = D = ab$, also nothwendig P_0' durch a theilbar, mithin $= ap'$ ist, $q_{-1}' = \frac{-c + ap'^2}{b}$ und $b^2q'_{-1} = - bc + acp'^2$.

Nach diesem Werthe von b^2q_{-1}' leuchtet sofort ein, dass da nach der dritten der Formeln (4) oder nach (15) $-bcRa$ ist, auch $b^2q_{-1}'Ra$ sein wird, und dass ferner, da nach der ersten der Formeln (4) oder nach (16) $abRc$ ist, auch $b^2q_{-1}'Rc$ sein wird. Demgemäss ist also auch der Bestand der Formel (24) konstatirt.

Hiernach bleibt kein Zweifel mehr übrig, dass die drei Formeln (4) oder (15), (16), (17) die nothwendigen und hinreichenden Bedingungen für die Lösbarkeit der Gleichung (1) darstellen.

VI. Wenn die beiden Koeffizienten auf der rechten Seite der gegebenen Gleichung (1) Primzahlen sind; so ist immer $a = 1$, also die dritte der Bedingungen (4) von selbst erfüllt. Für diesen Fall erfordert also die Lösbarkeit der Gleichung

(27) $$x^2 = by^2 + cz^2$$

nur die beiden Bedingungen

(28) bRc cRb

Nach der besonderen Form der beiden Primzahlen b und c gewähren aber die Sätze in §. 149, V. bis VIII. vom Bestande der Einen dieser beiden Bedingungen sofort einen Schluss auf den Bestand der anderen. Es genügt daher in diesen Fällen die Verwirklichung der Einen Bedingung, wennicht nach der besonderen Form von b und c die Gl. (27) allgemein unlösbar ist. Im Folgenden haben wir die hieraus sich ergebenden Resultate zusammengestellt, indem wir b stets als positiv, dagegen c bald als positiv, bald als negativ ansehen und für die absoluten

Werthe dieser Koeffizienten die verschiedenen Kombinationen der Primzahlen von der Form $4r+1$ und $4r+3$ unter einander, sowie auch die Kombinationen der Primzahlen von der Form $8r+1$, 3, 5, 7 mit der Primzahl 2 bilden.

wenn b	wenn c	so ist die Gleichung (27)
$4r+1$	$4s+1$	lösbar, wenn $(4r+1)R(4s+1)$
$4r+1$	$4s+3$	» » $(4r+1)R(4s+3)$
$4r+3$	$4s+1$	» » $(4r+3)R(4s+1)$
$4r+3$	$4s+3$	unlösbar
$4r+1$	$-(4s+1)$	lösbar, wenn $(4r+1)R(4s+1)$
$4r+1$	$-(4s+3)$	unlösbar
$4r+3$	$-(4s+1)$	»
$4r+3$	$-(4s+3)$	lösbar, wenn $(4r+3)R(4s+3)$
$4r+1$	-1	lösbar
$4r+3$	-1	unlösbar
$8r+1$	2	lösbar
$8r+7$	2	»
$8r+3$	2	unlösbar
$8r+5$	2	»
$8r+1$	-2	lösbar
$8r+3$	-2	»
$8r+5$	-2	unlösbar
$8r+7$	-2	»

Man erkennt leicht, dass durch diese und ähnliche Betrachtungen Verallgemeinerungen der Sätze des §. 156 gewonnen werden, indem z. B. nach dem Vorstehenden die Gleichung $x^2=(4r+1)y^2-z^2$ oder $x^2+z^2=(4r+1)y^2$ lösbar, dagegen die Gleichung $x^2+z^2=(4r+3)y^2$ unlösbar ist (vorausgesetzt, dass $4r+1$ und $4r+3$ Primzahlen seien). Demnach lässt sich jede Zahl von der Form $(4r+1)y^2$, aber keine Zahl von der Form $(4r+3)y^2$ in zwei Quadrate zerlegen, worin eine Verallgemeinerung des Fermatschen Satzes §. 156, I. besteht.

Allgemein ist die Gleichung $x^2=by^2-z^2$ oder $x^2+z^2=by^2$ dann lösbar, wenn $-1Rb$ ist, gleichviel ob b eine Primzahl sei oder nicht. Dagegen ist jene Gleichung unlösbar, wenn man $-1Nb$ hat. Der erstere Fall der Lösbarkeit tritt ein, wenn b aus lauter Primfaktoren von der Form $4r+1$ zusammengesetzt ist, wozu sich auch noch die Primzahl 2, jedoch nur auf erster Potenz gesellen darf (s. §. 150, IV., V., VI.).

Besitzt dagegen b einen Primfaktor von der Form $4r+3$ oder eine höhere Potenz von 2, als die erste; so ist jene Gleichung unmöglich. Demnach kann z. B. weder die Zahl $21=3.7$ noch eine Zahl von der Form $21y^2$ in zwei Quadrate zerlegt werden.

§. 164. **Beispiel:**

$$x^2=37y^2+44z^2$$

Diese Gleichung ist nach dem vorhergehenden Paragraphen lösbar. Denn der Koeffizient 37 von y^2 und der von seinem quadratischen Faktor 4 befreiete Koeffizient 11 von z^2, welche relativ prim sind, erfüllen die beiden Bedingungen, dass es Zahlen von der Form $37-p^2$ und $11-p^2$ gebe, welche resp. durch 11 und 27 theilbar sind, indem unter Anderem die erste Bedingung durch $p=2$ und die zweite durch $p=14$ verwirklicht ist.

Behuf der Auflösung nach §. 161 lassen wir vorläufig den Umstand, dass der Koeffizient von z^2 einen quadratischen Faktor enthält, ausser Acht und schreiben

$$x^2-37y^2=44z^2$$

Hierin ist $D=b=37$, $Q_0=c=44$, also $K=\frac{\sqrt{37}+P_0}{44}$. Jetzt sind die Reihen der durch 44 theilbaren Zahlen von der Form $37-P_0^2$ zu suchen. Man findet deren vier, für welche resp. $P_0=\pm 9, \pm 13$ ist. Nimmt man einmal $P_0=13$; so hat man $K=\frac{\sqrt{37}+13}{44}$, und Dies gibt die Entwickelung

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
-2					0	1
-1		-3	3		1	0
0	13	44	12	0	0	1
1	-13	-3	3	2	1	2
2	7	4	4	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

welche bei dem Zeiger $m=2$ abgebrochen werden kann, da hierfür $(-1)^m Q_m=(-1)^2 Q_2=4$ ein vollkommenes Quadrat ist. Für diesen Werth von m hat man ferner $P_m=7$, $Q_m=4$, $M_{m-1}=1$, $N_{m-1}=2$, $M_{m-2}=0$, $N_{m-2}=1$. Die transformirte Gleichung, welche an die Stelle der Gl. (14) in §. 161 tritt, ist

$$x'^2-4y'^2=37z'^2$$

Dieselbe kann nach §. 160, III. aufgelös't werden, und gibt, wenn p, q irgend zwei Faktoren bezeichnen, in welchen sich die Zahl 37 zerlegen lässt, sodass man also

$$p = 1 \quad 37 \quad -1 \quad -37$$
$$q = 37 \quad 1 \quad -37 \quad -1$$

hat,

$$x' = \frac{u}{2}(pv^2 + qw^2), \qquad y' = \frac{u}{4}(pv^2 + qw^2), \qquad z' = uvw$$

Wie schon früher bemerkt, ist es bequemer, nicht sofort diese Werthe von x', y', z' in die Formeln des §. 161 einzuführen, sondern die Auflösung x, y, z der gegebenen Gleichung erst mittelst der einfachen Zeichen x', y', z' darzustellen. Zu diesem Ende hat man nach der Gruppe (G) von Gleichungen in §. 161

$$\mathfrak{M}_n = \frac{x' + P_m z'}{Q_m} = \frac{x' + 7z'}{4}, \qquad \mathfrak{U}_n = z'$$

$$M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{U}_2 = 1 \,.\, \frac{x' + 7z'}{4} + 0 \,.\, z' = \frac{x' + 7z'}{4}$$

$$N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{U}_n = 2 \,.\, \frac{x' + 7z'}{4} + 1 \,.\, z' = \frac{x' + 9z'}{2}$$

$$x = Q_0 M_{m+n} - P_0 N_{m+n} = 44 \,.\, \frac{x' + 7z'}{4} - 13 \,.\, \frac{x' + 9z'}{2} = \frac{9x' + 37z'}{2}$$

$$y = N_{m+n} = \frac{x' + 9z'}{3}, \qquad z = y'$$

Jetzt hat man also die Werthe von x, y, z, ausgedrückt durch x', y', z', gefunden. Substituirt man für die letzteren Grössen ihre aus der transformirten Gleichung sich ergebenden Werthe; so erhält man

$$x = \frac{u}{4}[9(pv^2 + qw^2) + 74vw]$$

$$y = \frac{u}{4}(pv^2 + qw^2 + 18vw)$$

$$z = \frac{u}{4}(pv^2 - qw^2)$$

Hierin bleiben v, w ganz willkürlich, und u ist so zu nehmen, dass x, y, z ganze Zahlen werden, was offenbar für jedes Vielfache von 4 geschehen würde.

Nähme man einmal $p = 1$, $q = 37$, $v = 1$, $w = 0$, $u = 4$; so ergäben sich die Werthe $x = 9$, $y = 1$, $z = 1$.

Jetzt würde die Auflösung der gegebenen Gleichung noch für die drei anderen Werthe von $P_0 = -13$, 9, -9 zu bewirken sein, was wir hier übergehen.

Ausserdem ist wegen des quadratischen Faktors 4, welchen die Grösse $Q_0 = 44 = 2^2 . 11$ besitzt, nach §. 161, VII. die Gleichung

$$x_1^2 - 37y_1^2 = 11z_1^2$$

zu behandeln, für welche $D=37$, $Q_0=11$, also $K=\frac{\sqrt{37}+P_0}{11}$ ist. Für die Reihen der durch 11 theilbaren Zahlen von der Form $37-P_0^2$ hat man $P_0=\pm 2$. Nimmt man einmal $P_0=-2$; so hat man für $K=\frac{\sqrt{37}-2}{11}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
−2					0	1
−1		3	−3		1	0
0	−2	11	11	0	0	1
1	2	3	−3	2	1	2
2	4	7	7	1	1	3
3	3	4	−4	2	3	8
4	5	3	3	3	10	27
5	4	7	−7	1	13	35
6	3	4	4	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Hier kann man bei $m=6$ schliessen, indem man $(-1)^6 Q_6=4$ hat. Es ist dann $P_m=3$, $Q_m=4$, $M_{m-1}=13$, $N_{m-1}=35$, $M_{m-2}=10$, $N_{m-2}=27$, und als reduzirte Gleichung hat man

$$x'^2-4y'^2=37z'^2$$

Diese reduzirte Gleichung ist ebenso gebildet, wie die frühere. Sie hat also auch die oben angegebenen Auflösungen für x', y', z'. Die Gruppe (G) in §. 161 liefert dann

$$\mathfrak{M}_n=\frac{x'-3z'}{4},\qquad \mathfrak{N}_n=x'$$

$$M_{m+n}=13.\frac{x'+3z'}{4}+10.z'=\frac{13x'+79z'}{4}$$

$$N_{m+n}=35.\frac{x'+3z'}{4}+27.z'=\frac{35x'+213z'}{4}$$

$$x_1=11.\frac{13x'+79z'}{4}-(-2).\frac{35x'+213z'}{4}=\frac{213x'+1295z'}{4}$$

$$y_1=\frac{35x'+213z'}{4},\qquad z_1=y'$$

Substituirt man hierin für x', y', z' ihre Werthe aus der transformirten Gleichung, und beachtet, dass jetzt $x=2x_1$, $y=2y_1$, $z=z_1$ ist; so kommt

$$x=2x_1=\frac{u}{4}[213(pv^2+qw^2)+2590vw]$$

$$y=2y_1=\frac{u}{4}[35(pv^2+qw^2)+426vw]$$

$$z=z_1=\frac{u}{4}(pv^2-qw^2)$$

Unter Anderem ergeben $p = 1$, $q = 37$, $v = 1$, $w = 0$, $u = 4$ die Werthe $x = 213$, $y = 35$, $z = 1$. Hierin besitzen zwar die beiden Grössen x und y nicht, wie es nach §. 161, VII. zu erwarten wäre, das gemeinschaftliche Maass 2; Dies hat jedoch darin seinen Grund, dass man nicht dafür gesorgt hat, dass die Auflösungen x_1, y_1, z_1 ganze Zahlen sind. Unter solchen Umständen repräsentiren die vorstehenden Formeln für x, y, z eine grössere Anzahl von Auflösungen, welche zum Theil der Kategorie derjenigen angehören, bei welchen man den quadratischen Faktor von 44 nicht ausscheidet.

§. 165. **Beispiel:**

$$x^2 = 528y^2 - 618z^2$$

In dieser Gleichung hat $528 = 16.33$ den quadratischen Faktor 16. Nach Ausscheidung desselben besitzen $33 = 3.11$ und $618 = 3.206$ das grösste gemeinschaftliche Maass 3 und die Gleichung wird lösbar sein, wenn es nach §. 163 Zahlen von der Form $33 - p^2$, $-618 - p^2$, $2266 - p^2$ gibt, welche resp. durch 206, 11, 3 theilbar sind.

Da diese Bedingungen resp. für $p = 41$, 3, 1 erfüllt sind; so ist die gegebene Gleichung lösbar. Schreiben wir dieselbe

$$x^2 - 528y^2 = -618z^2$$

so ist $D = 528$, $Q_0 = -618$, $K = \frac{\sqrt{528} + P_0}{-618}$. Unter den Werthen von P_0, für welche $528 - P_0^2$ durch 618 theilbar wird, findet man auch $P_0 = \pm 42$. Nimmt man $P_0 = 42$; so hat man für $K = \frac{\sqrt{528} + 42}{-618}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
—2					0	1
—1		2	—2		1	0
0	42	—618	—618	—1	—1	1
1	576	536	—536	1	0	1
2	—40	—2	—2	8	—1	9
3	24	24	—24	1	—1	10
4	0	22	22	1	—2	19
5	22	2	—2	22	—45	428
6	22	22	22	2	—92	875
7	22	2	—2	:	:	:
:	:	:	:	:	:	:

In dieser Entwickelung kommt unter den Grössen $(-1)^m Q_m$ kein Quadrat vor. Der kleinste positive Werth darunter ist 22; wir wollen jedoch den kleinsten negativen Werth -2

auswählen, da derselbe bedeutend kleiner ist, als jener. Da dieser Werth -2 nicht bloss in der Periode, sondern auch schon früher vorkommt; so wollen wir denselben bei dem Zeiger $m=2$ nehmen. Dies giebt $(-1)^m Q_m = -2$, $Q_m = -2$, $P_m = -40$, $M_{m-1} = 0$, $N_{m-1} = 1$, $M_{m-2} = -1$, $N_{m-2} = 1$ und man hat die transformirte Gleichung

$$x'^2 - (-2)y'^2 = 528z'^2$$

Hierin ist $D' = -2$, $Q_0' = 528$, also $K' = \frac{\sqrt{-2} + P_0'}{528}$. Es sind jetzt die durch 528 theilbaren Zahlen von der Form $-2 - P_0'^2$ zu suchen. Da $528 = 3 \,.\, 11 \,.\, 16$ ist und es keine durch 16 theilbare Zahl von der Form $-2 - P_0'^2$ gibt; so kann es auch keine durch 528 theilbare Zahl von dieser Form geben.

Wir können also bei dem angenommenen Werthe von $P_0 = 42$ nur noch untersuchen, ob diese transformirte Gleichung auflösbar ist, nachdem rechts der quadratische Faktor $16 = 4^2$ abgesondert ist, also wenn man nach §. 161, VII.

$$x_1'^2 - (-1)y_1'^2 = 33z_1'^2$$

schreibt. Hierin hat man $D' = -2$, $Q_0' = 33$, $K' = \frac{\sqrt{-2} + P_0'}{23}$, und es kann $P_0' = \pm 8$, ± 14 genommen werden. Nimmt man $P_0' = 8$; so kommt für $K' = \frac{\sqrt{-2} + 3}{33}$

m'	$P'_{m'}$	$Q'_{m'}$	$(-1)^{m'} Q'_{m'}$	$a'_{m'}$	$M'_{m'}$	$N'_{m'}$
-2					0	1
-1		-2	2		1	0
0	8	33	33	0	0	1
1	-8	-2	2	4	1	4
2	0	1	1	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Hier kann man schliessen bei $m' = 2$, $(-1)^{m'} Q'_{m'} = 1$, $P'_{m'} = 0$, $Q'_{m'} = 1$, $M'_{m'-1} = 1$, $N'_{m'-1} = 4$, $M'_{m'-2} = 0$, $N'_{m'-2} = 1$. Die zweite transformirte Gleichung ist nun

$$x''^2 - 1 \,.\, y''^2 = -2z''^2$$

Dieselbe kann nach §. 160, III. aufgelös't werden, und indem $pq = -2$ ist, hat man

$$x'' = \frac{u}{2}(pv^2 + qw^2), \qquad y'' = \frac{u}{2}(pv^2 - qw^2), \qquad z'' = uvw$$

Die rückwärts gehenden Substitutionen liefern nun nach der in §. 161 bezeichneten Gruppe (G'), welche mit der Gruppe (G) bis auf die Anzahl der Akzente genau übereinstimmt,

$$\mathfrak{M}'_{n'} = \frac{x'' + 0 \,.\, z''}{1} = x'', \qquad \mathfrak{N}'_{n'} = z''$$

$$M'_{m'+n'} = 1 \,.\, x'' + 0 \,.\, z'' = x'', \quad N'_{m'+n'} = 4 \,.\, x'' + 1 \,.\, z'' = 4x'' + z''$$

$$x_1' = 33 x'' - 8(4x'' + z'') = x'' - 8z'', \quad y_1' = 4x'' + z'', \quad z_1' = y''$$

Hiernach ist

$$x' = 4x_1' = 4x'' - 32z'', \quad y' = 4y_1' = 16x'' + 4z'', \quad z' = z_1' = y''$$

ferner nach der Gruppe (G)

$$\mathfrak{M}_n = \frac{x' + (-40)z'}{-2} = -2x'' + 20y'' + 16z'', \quad \mathfrak{N}_n + z' = y''$$

$$M_{m+n} = 0 \,.\, (-2x'' + 20y'' + 16z'') + (-1) \,.\, y'' = -y''$$

$$N_{m+n} = 1 \,.\, (-2x'' + 20y'' + 16z'') + 1 \,.\, y'' = -2x'' + 21y'' + 16z''$$

$$x = -618 \,.\, (-y'') - 42 \,.\, (-2x'' + 21y'' + 16z'')$$
$$= 12(7x'' - 22y'' - 56z'')$$

$$y = -2x'' + 21y'' + 16z'', \qquad z = 16x'' + 4z''$$

Substituirt man hierin die obigen Werthe von x'', y'', z''; so kommt

$$x = 6u(-15pv^2 + 29qw^2 - 112vw)$$

$$y = \frac{u}{2}(19pv^2 - 23qw^2 + 32vw)$$

$$z = 4u(2pv^2 + 2qw^2 + vw)$$

Nimmt man einmal $p = 1$, $q = -2$, $v = 1$, $w = 0$, $u = 2$; so ergeben sich die Werthe $x = -180$, $y = 19$, $z = 16$.

Um für das vorstehende Beispiel die Schlussbemerkung VIII. aus §. 161 in Anwendung zu bringen, also eine Grösse $(-1)^{m+n+1} Q_{m+n+1}$ aus der Entwickelung von $K = \frac{\sqrt{528} + 42}{-618}$ darzustellen, welche ein vollkommenes Quadrat ist; so hat man für die letzteren speziellen Werthe $x = -180$, $y = 19$, $z = 16$,

$$\frac{M_{m+n}}{N_{m+n}} = \frac{x + P_0 y}{Q_0 y} = \frac{-180 + 42 \,.\, 19}{-618 \,.\, 19} = \frac{1}{-19} = [0, -19]$$

Entwickelt man nun K nach den beiden Quotienten 0, -19; so kommt in der That

m	P_m	Q_m	$(-1)_m Q_m$	a_m	M_m	N
-2					0	1
-1		2			1	0
0	42	-618	-618	0	0	1
1	-42	2	-2	-19	1	-19
2	4	256	256			

und es ist wirklich $(-1)^2 Q_2 = 256 = 16^2$ ein vollkommenes Quadrat.

§. 166. **Beispiel:**

$$x^2 = 13y^2 - 139z^2$$

An diesem Beispiele, welches sich in den Zusätzen von Lagrange zu Eulers Algebra, §. 56, vorfindet, wollen wir zeigen, in welchem Grade sich unsere Methode gegen die von Lagrange durch Kürze empfiehlt. Dabei machen wir darauf aufmerksam, dass die Schwierigkeiten der Einen und der anderen Methode nicht in den dabei vorkommenden Substitutionen, sondern vorzugsweise in den Nebenrechnungen bestehen, welche jeder Übergang von Einer transformirten Gleichung zu der nächstfolgenden erfordert, namentlich in der Aufsuchung der durch Q theilbaren Zahlen von der Form $D - P^2$. Diese Operationen werden aber durch unsere Methode dadurch auf das Äusserste beschränkt, dass man den Koeffizienten für die nächste transformirte Gleichung aus mehreren anderen auswählen kann, worunter sich oftmals schon ein Quadrat und in jedem Falle eine bedeutend kleinere Zahl vorfindet. Nach dem Verfahren von Lagrange muss man sich jedoch mit dem einzigen Koeffizienten begnügen, welcher sich durch die a. a. O. nachzusehende Rechnung darbietet. Dies kann unter Umständen schon bei mässigen Koeffizienten eine sehr grosse Anzahl von Transformationen nach sich ziehen, während unsere Methode nach §. 162 selbst bei grossen Koeffizienten doch nur wenige Transformationen erheischt.

Um die obige Gleichung nach unserer Methode aufzulösen, schreiben wir dieselbe

$$x^2 - 13y^2 = -139z^2$$

Es ist $D = 13$, $Q_0 = -139$, $K = \frac{\sqrt{13} + P_0}{-139}$. Sucht man die durch 139 theilbaren Zahlen von der Form $13 - P_0^2$; so findet man unter Anderem $P_0 = 41$. Hierfür wird $K = \frac{\sqrt{13} + 41}{-139}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
−2					0	1
−1		12	−12		1	0
0	41	−139	−139	−1	−1	1
1	98	69	−69	1	0	1
2	−29	−12	−12	2	−1	3
3	5	1	−1	8	−8	25
4	3	4	4	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Man kann hier nehmen $m = 4$, $(-1)^m Q_m = 4$, $Q_m = 4$, $P_m = 3$; $M_{m-1} = -8$, $N_{m-1} = 25$, $M_{m-2} = -1$, $N_{m-2} = 3$. Die erste transformirte Gleichung

$$x'^2 - 4y'^2 = 13z'^2$$

ist auch die Sclussgleichung, und man hat, wenn $pq = 13$ ist, nach §. 160

$$x' = \frac{u}{2}(pv^2 + qw^2), \quad y' = \frac{u}{4}(pv^2 - qw^2), \quad z' = uvw$$

Die Gruppe (G) aus §. 161 liefert

$$\mathfrak{M}_n = \frac{x' + 3z'}{4}, \qquad \mathfrak{N}_n = z'$$

$$M_{m+n} = -8 \cdot \frac{x' + 3z'}{4} - 1 \cdot z' = -2x' - 7z'$$

$$N_{m+n} = 25 \cdot \frac{x' + 3z'}{4} + 3 \cdot z' = \frac{25x' + 87z'}{4}$$

$$x = -139 \cdot (-2x' - 7z') - 41 \cdot \frac{25x' + 87z'}{4} = \frac{87x' + 325z'}{4}$$

$$y = \frac{25x' + 87z'}{4}, \qquad z = y'$$

und wenn man hierin für x', y', z' ihre obigen Werthe einführt,

$$x = \frac{u}{8}[87(pv^2 + qw^2) + 650vw]$$

$$y = \frac{u}{8}[25(pv^2 + qw^2) + 174vw]$$

$$z = \frac{u}{4}(pv^2 - qw^2)$$

So hat man z. B. für $p = 1$, $q = 13$, $v = 1$, $w = 0$, $u = 8$ die Werthe $x = 87$, $y = 25$, $z = 2$.

Vergleicht man diese Rechnung mit der von Lagrange eingeschlagenen; so findet man, dass derselbe zunächst zu dem Koeffizienten -12 und demnach zu der ersten transformirten Gleichung $x'^2 + 12y'^2 = 13z'^2$ gelangt. Diese muss wieder wie die gegebene behandelt werden, wobei Lagrange den quadratischen Faktor des Koeffizienten 12 beseitigt und $x'^2 + 3y_1'^2 = 13z'^2$ schreibt. Aber die Methode von Lagrange verstattet noch nicht einmal, dass die Rechnung in der jetzt folgenden Entwickelungsstufe, bei welcher die durch 13 theilbaren Zahlen von der Form $-3 - P_0'^2$ zu suchen sind, schliesse, vielmehr führt die neue Rechnung erst zu einer zweiten transformirten Gleichung $x''^2 - 3y''^2 = -3z''^2$. Mit dieser Gleichung ist nun nochmals wie mit der gegebenen zu verfahren, und Dies erst führt zu der Schlussgleichung. Die Methode von Lagrange erfordert also hier drei Transformationen, während es bei der unserigen mit einer einzigen abgethan ist.

§. 167. Verallgemeinerung der Auflösungsmethode des §. 161, sodass darunter auch die Behandlung der Gleichungen des §. 160 begriffen ist.

Die Methode des §. 161 gewinnt, wennauch nicht an Kürze, doch an Eleganz und wissenschaftlicher Vollkommenheit, wenn die in §. 160 vorgetragene eigenthümliche Auflösung der in der Form $x^2 - \beta^2 y^2 = cz^2$ erscheinenden Schlussgleichung, wobei man wegen der Zerlegung des Koeffizienten c in Faktoren sogar noch ein anderes Problem der unbestimmten Analytik in Anspruch nehmen muss, durch eine ganz im Geiste der Transformationen liegende Operation ersetzt wird. Dies kann folgendermaassen geschehen.

Behandeln wir die Gleichung

(1) $$x^2 - \beta^2 y^2 = \pm cz^2$$

genau so, wie es in §. 161 behuf der dortigen Transformation vorgeschrieben ist; so haben wir $D = \beta^2$, $Q_0 = c$, $K = \frac{\sqrt{\beta^2} + P_0}{c}$. Es sind also auch hier die Reihen der durch c theilbaren Zahlen von der Form $D - P_0^2 = \beta^2 - P_0^2$ aufzusuchen. Da aber jetzt die Determinante $D = \beta^2$ ein Quadrat ist; so weiss man aus §. 87 ff., dass man unter den Grössen Q_n den Werth 0 erzeugen kann. Diesen Werth nehmen wir für Q_m; es sei also $Q_m = 0$ und $P_m = \pm\beta = \sqrt{D}$ (§. 87). Alsdann können wir aber nicht die Gl. (6) in §. 161, welche aus der Gl. (5) in §. 124 nach vorgängiger Multiplikation mit Q_m entstanden ist, in Anwendung bringen, da dieselbe die identische Beziehung $0 = 0$ ergeben würde; vielmehr ist die Gl. (5) in §. 124 in ihrer ursprünglichen Form, aber mit den Bezeichnungen des §. 161 zu verwenden. Hiernach hat man

(2) $$-2P_m\mathfrak{M}_n\mathfrak{N}_n - Q_{m-1}\mathfrak{N}_n^2 = (-1)^m(-1)^{m+n+1}Q_{m+n+1}$$

Nach der in §. 161 gemachten Voraussetzung soll nun $(-1)^{m+n+1}Q_{m+n+1} = z^2$ ein vollkommenes Quadrat sein. Schreibt man also dafür den Werth $u^2v^2w^2$; so kann man Gl. (2) in die Form

(3) $$-\mathfrak{N}_n(2P_m\mathfrak{M}_n - Q_{m-1}\mathfrak{N}_n) = (-1)^m u^2v^2w^2 = uv^2 . (-1)^m uw^2$$

bringen, und hieraus folgt

(4) $$\mathfrak{N}_n = uv^2, \quad \text{und} \quad -(2P_m\mathfrak{M}_n + Q_{m-1}\mathfrak{N}_n) = (-1)^m uw^2, \quad \text{also}$$

(5) $$\mathfrak{M}_n = \frac{u[Q_{m-1}v^2 + (-1)^m w^2]}{-2P_m}$$

Die Grössen u, v, w bleiben willkürlich; sie sind jedoch so zu wählen, dass $\mathfrak{M}_n$ eine ganze Zahl wird, auch dass die beiden Grössen $\mathfrak{M}_n$ und $\mathfrak{N}_n$, welche den Zähler und Nenner eines reduzirten Kettenbruchs darstellen, relativ prim werden. Man findet übrigens leicht, dass nach der Natur der gegebenen

Gleichung von der Strenge dieser Bedingungen abgesehen werden kann. Es ist nämlich auch statthaft, dass $\mathfrak{M}_n$ und $\mathfrak{N}_n$ ein gemeinschaftliches Maass besitzen, und es genügt, u, v, w so zu bestimmen, dass die Auflösungen x, y, z der ursprünglich gegebenen Gleichung, wovon die obige Gleichung (1) irgend eine transformirte ist, ganze Zahlwerthe annehmen.

Von den Werthen (4) und (5) für $\mathfrak{M}_n$ und $\mathfrak{N}_n$ und dem Werthe

(6) $$z = uvw$$

steigt man nun durch die Gruppe (G) des §. 161 auf zu den rückwärts liegenden Gleichungen. Die nächste Gleichung, deren Auflösung man auf diese Weise erhält, ist die vorstehende Gl. (1), und zwar hat man hierfür, nachdem M_{m+n} und N_{m+n} bestimmt sind,

(7) $$x = Q_0 M_{m+n} - P_0 N_{m+n}, \quad y = N_{m+n}, \quad z = uvw$$

Man erkennt, dass man durch das vorstehende Verfahren auch der Prüfung überhoben wird, ob sich unter den Grössen Q der Entwickelungen von K, K', K'' ... Quadrate vorfinden. Wenn man immer das kleinste Q zur nächsten Determinante wählt, wird man bei irgend einer Entwickelung immer auf den Werth $Q = 0$ stossen müssen, welcher anzeigt, dass die dieser Entwickelung zu Grunde liegende Determinante ein Quadrat ist, und dass man sich also in einem Falle der soeben beschriebenen Art befindet.

Beispiel. In dem Beispiele des §. 166 stiessen wir auf die transformirte Gleichung

$$x^2 - 4y^2 = 13z^2$$

Behandeln wir dieselbe in vorstehender Weise; so ist $D = 4$, $Q_0 = 13$, $K = \frac{\sqrt{4} + P_0}{13}$. Es gibt hier zwei Reihen der durch 13 theilbaren Zahlen von der Form $4 - P_0^2$, wofür man $P_0 = \pm 2$ hat. Nimmt man $P_0 = 2$; so kommt $K = \frac{\sqrt{4} + 2}{13}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
-2					0	1
-1		0	0		1	0
0	2	13	13	0	0	1
1	-2	0	0	3	1	3

Hier kann man sofort $m = 1$, $Q_m = 0$, $P_m = -2$, $Q_{m-1} = 13$, $M_{m-1} = 0$, $N_{m-1} = 1$, $M_{m-2} = 1$, $N_{m-2} = 0$ nehmen. Dies gibt nach Gl. (5) und (4)

$$\mathfrak{M}_n = \frac{u}{4}(13v^2 - w^2), \qquad \mathfrak{N}_n = uv^2$$

und dann nach der Gruppe (G) in §. 161

$$M_{m+n} = 0 \,.\, \frac{u}{4}(13v^2 - w^2) + 1 \,.\, uv^2 = uv^2$$

$$N_{m+n} = 1 \,.\, \frac{u}{4}(13v^2 - w^2) + 0 \,.\, uv^2 = \frac{u}{4}(13v^2 - w^2)$$

$$x = 13 \,.\, uv^2 - 2 \,.\, \frac{u}{4}(13v^2 - w^2) = \frac{u}{2}(13v^2 + w^2)$$

$$y = \frac{u}{4}(13v^2 - w^2)$$

$$z = uvw$$

§. 168. *Auflösung der Gleichung:*

(1) $ax^2 - by^2 = cz^2$ oder $ax^2 = by^2 + cz^2$

worin, wenn b und c gleiche Zeichen haben sollten, a dasselbe Zeichen besitze, indem im entgegengesetzten Falle nur die Auflösung $x = 0$, $y = 0$, $z = 0$ möglich sein würde.

I. Ist a ein Quadrat $= \alpha^2$; so schreibt man diese Gleichung

(2) $(\alpha x)^2 = X^2 = by^2 + cz^2$

lös't dieselbe für X, y, z nach §. 161 auf, und indem man schliesslich

(3) $x = \dfrac{X}{\alpha}$

setzt, bestimmt man die Willkürliche u so, dass x, y, z ganze Zahlen werden.

II. Ist a kein Quadrat (und überhaupt keiner der Koeffizienten a, b, c der positive oder negative Werth eines Quadrates); so geht die Gl. (1) durch Multiplikation mit a in die Form

(4) $(ax)^2 = X^2 = aby^2 + acz^2$

über. Diese Gleichung ist wie (2) nach §. 161 aufzulösen, indem man schliesslich

(5) $x = \dfrac{X}{a}$

setzt.

III. Wenn a einen quadratischen Faktor enthält, wenn also die gegebene Gleichung die Form

(6) $a\alpha^2x^2 = by^2 + cz^2$

hat; so gereicht es der Rechnung zur Abkürzung, wenn man

nicht mit dem ganzen Koeffizienten von x^2, sondern nur mit dem nicht quadratischen Faktor a desselben multiplizirt. Dies gibt

$$(7) \qquad (a\alpha x)^2 = X^2 = aby^2 + acz^2$$

$$(8) \qquad x = \frac{X}{a\alpha}$$

IV. Um von vorn herein die Lösbarkeit der gegebenen Gleichung (1) zu prüfen, kann man, wie schon in §. 163 bemerkt ist, die etwaigen quadratischen Faktoren der Koeffizienten a, b, c ausser Acht lassen.

Hätten alle drei Koeffizienten ein gemeinschaftliches Maass; so werde dasselbe, da es auf die Werthe von x, y, z gar keinen Einfluss ausübt, und nur die Rechnung durch unnöthig grosse Zahlen beschwert, durch Division beseitigt.

Hätten aber irgend zwei jener Koeffizienten ein gemeinschaftliches Maass; so könnte man die ganze Gleichung damit multipliziren. Hierdurch entständen in den betreffenden beiden Gliedern quadratische Faktoren, welche bei der gegenwärtigen Untersuchung ausgeschieden werden können.

Demnach kann man bewirken, dass von den Koeffizienten a, b, c keiner einen quadratischen Faktor enthalte, und keine zwei ein gemeinschaftliches Maass besitzen.

Multiplizirt man unter dieser Voraussetzung die Gl. (1) mit a; so erhält man die Form (4), und für die Lösbarkeit der Letzteren hat man nach §. 163 (4) die drei Bedingungen

$$(9) \qquad abRc, \qquad acRb, \qquad -bcRa$$

Wäre die zu untersuchende Gleichung in der Form

$$(10) \qquad ax^2 + by^2 + cz^2 = 0$$

gegeben; so würden diese Bedingungen, wie leicht zu erachten, in folgende Form übergehen

$$(11) \qquad -abRc, \qquad -acRb, \qquad -bcRa$$

§. 169. **Beispiel:**

$$7x^2 - 15y^2 + 23z^2 = 0$$

Dieses Beispiel hat Gauss nach seiner eigenen Methode, welche von der des Lagrange ganz verschieden ist, in den *Disq. arithm. art. 294* behandelt. Um dasselbe nach unserer Methode aufzulösen, multipliziren wir mit 7 und schreiben, indem wir $7x = X$ setzen,

$$X^2 - 105y^2 = -161z^2$$

Hierin ist $D = 105$, $Q_0 = -161$, $K = \frac{\sqrt{105} + P_0}{-161}$. Um die

durch 161 theilbaren Zahlen von der Form $105 - P_0^2$ aufzusuchen, beachte man, dass $161 = 7.23$ ist, und suche einzeln die durch 7 und die durch 23 theilbaren Zahlen. Man findet die beiden Werthe $P_0 = \pm 63$. Nimmt man $P_0 = 63$; so kommt

$$K = \frac{\sqrt{105} + 63}{-161}$$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
—2					0	1
—1		24	—24		1	0
0	63	—161	—161	—1	—1	1
1	98	59	—59	1	0	1
2	—39	—24	—24	1	—1	2
3	15	5	—5	5	—5	11
4	10	1	1	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Hier kann man nehmen $m = 4$, $(-1)^m Q_m = 1$, $P_m = 10$, $Q_m = 1$, $M_{m-1} = -5$, $N_{m-1} = 11$, $M_{m-2} = -1$, $N_{m-2} = 2$. Die transformirte Gleichung ist

$$x'^2 - y'^2 = 105 z'^2$$

Dieselbe kann nach §. 160 aufgelös't werden und gibt, wenn $pq = 105$ ist,

$$x' = \frac{u}{2}(pv^2 + qw^2), \qquad y' = \frac{u}{2}(pv^2 - qw^2), \qquad z' = uvw$$

Nach der Gruppe (G) aus §. 161 hat man nun

$$\mathfrak{M}_n = x' + 10z', \quad \mathfrak{N}_n = z'$$

$$M_{m+n} = -5.(x' + 10z') + (-1).z' = -5x' - 51z'$$

$$N_{m+n} = 1.(x' + 10z') + 2.z' = 11x' + 112z'$$

$$X = -161.(-5x' - 51z') - 63.(11x' + 112z') = 7(16x' + 165z')$$

$$y = 11x' + 112z', \qquad z = y'$$

Substituirt man hierin die obigen Werthe von x', y', z'; so kommt

$$x = \frac{X}{7} = u\,[8(pv^2 + qw^2) + 165vw]$$

$$y = \frac{u}{2}[11(pv^2 + qw^2) + 224vw]$$

$$z = \frac{u}{2}(pv^2 - qw^2)$$

So erhält man z. B. für $p = 1$, $q = 105$, $v = 1$, $w = 0$, $u = 2$ die Werthe $x = 16$, $y = 11$, $z = 1$.

§. 170. **Auflösung der Gleichung:**

(1) $$ax^2 - 2bxy - cy^2 = kz^2$$

Es wird vorausgesetzt, dass der Koeffizient des Gliedes xy zu einer paaren Zahl gemacht sei. Multiplizirt man mit a und addirt auf der linken Seite die Glieder $b^2y^2 - b^2y^2$; so lässt sich die vorstehende Gleichung in die Form

$$(ax - by)^2 - (b^2 + ac)y^2 = akz^2$$

oder wenn man

(2) $$ax - by = X$$

setzt, in die Form

(3) $$X^2 - (b^2 + ac)y^2 = akz^2.$$

bringen, welche die reduzirte Gleichung darstellt. Lös't man diese Gleichung nach §. 161 für X, y, z auf; so hat man schliesslich wegen der Beziehung (2)

(4) $$x = \frac{X + by}{a}$$

zu nehmen, und der Vollständigkeit wegen ist zu beachten, dass hierin die aus der Gl. (3) sich ergebenden Grössen X und y unabhängig von einander sowol positiv wie negativ genommen werden können.

Beispiel: $$2x^2 + 6xy - 5y^2 = 3z^2$$

Die reduzirte Gleichung wird hier, wo $b^2 + ac = 3^2 + 2.5 = 19$ ist,

$$X^2 - 19y^2 = 6z^2$$

indem man nach Gl. (4) $x = \frac{X - 3y}{2}$ hat. Um dieselbe aufzulösen, schreiben wir sie in der Form

$$X^2 - 6Y^2 = 19Z^2$$

worin wir nur wegen der Übereinstimmung mit der früheren Buchstabenfolge Y und Z resp. an die Stelle von z und y gesetzt haben.

Jetzt ist $D = 6$, $Q_0 = 19$, $K = \frac{\sqrt{6} + P_0}{19}$. Man hat $P_0 = \pm 5$.

Für den Werth $P_0 = 5$ ergibt sich $K = \frac{\sqrt{6} + 5}{19}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
-2					0	1
-1		-1	1		1	0
0	5	19	19	0	0	1
1	-5	-1	1	⋮	⋮	⋮
⋮	⋮	⋮	⋮			

Man kann hier nehmen $m=1$, $(-1)^m Q_m = 1$, $P_m = -5$, $Q_m = -1$, $M_{m-1} = 0$, $N_{m-1} = 1$, $M_{m-2} = 1$, $N_{m-2} = 0$. Die transformirte Gleichung ist

$$x'^2 - y'^2 = 6z'^2$$

und dieselbe gibt nach §. 160, indem $pq=6$ ist,

$$x' = \frac{u}{2}(pv^2 + qw^2), \quad y' = \frac{u}{2}(pv^2 - qw^2), \quad z' = uvw$$

Ferner ist nach der Gruppe (G) in §. 160

$$\mathfrak{M}_n = \frac{x' - 5z'}{-1} = -x' + 5z', \quad \mathfrak{N}_n = z'$$

$$M_{m+n} = 0.(-x' + 5z') + 1.z' = z'$$

$$N_{m+n} = 1(-x' + 5z') + 0.z' = -x' + 5z'$$

$$X = 19.z' - 5(-x' + 5z') = 5x' - 6z'$$

$$Y \text{ oder } z = -x' + 5z', \qquad Z \text{ oder } y = y'$$

und hiernach hat man

$$x = \frac{X - 3y}{2} = \frac{5x' - 3y' - 6z'}{2}$$

Substituirt man in diese Ausdrücke von x, y, z die obigen Werthe von x', y', z'; so ergibt sich

$$x = \frac{u}{2}(pv^2 + 4qw^2 - 6vw)$$

$$y = \frac{u}{2}(pv^2 - qw^2)$$

$$z = \frac{u}{2}(-pv^2 - qw^2 + 10vw)$$

So erhält man z. B. für $p=3$, $q=2$, $v=1$, $w=1$, $u=2$ die Werthe $x=5$, $y=1$, $z=5$.

§. 171. *Spezielle Fälle der vorstehend behandelten Gleichung.*

I. Wenn in der Gleichung des vorhergehenden Paragraphen das mit dem Quadrate der Einen Unbekannten y behaftete Glied fehlt, also $c=0$ ist; so braucht nicht nothwendig der Koeffizient des in xy multiplizirten Gliedes paar zu sein. Wäre also gegeben

$$(1) \qquad ax^2 + bxy = kz^2$$

so kann man $pq = k$, $z = uvw$ und

$$x(ax + by) = upv^2 . uqw^2$$

setzen, woraus sofort die Auflösung

$$(2) \qquad x = upv^2, \qquad y = \frac{u}{b}(qw^2 - apv^2), \qquad z = uvw$$

folgt. Die gegebene Gleichung ist also immer lösbar.

Beispiel: $3x^2 + 10xy = 7z^2$

Hier ist $pq = 7$ und

$$x = upv^2, \quad y = \frac{u}{10}(qw^2 - 3pv^2), \quad z = uvw$$

So ergeben sich für $p = 1$, $q = 7$, $v = 1$, $w = 3$, $u = 1$ die Werthe $x = 1$, $y = 6$, $z = 3$.

II. Fehlte auch das Quadrat von x, wäre also auch $a = 0$ und

(3) $$bxy = kz^2$$

so ergibt sich für $pq = k$ die Auflösung

(4) $$x = upv^2, \quad y = \frac{uqw^2}{b}, \quad z = uvw$$

Beispiel: $5xy = 6z^2$

Hier ist $pq = 6$ und

$$x = upv^2, \quad y = \frac{uqw^2}{5}, \quad z = uvw$$

Nimmt man einmal $p = 2$, $q = 3$, $v = 1$, $w = 5$, $u = 1$; so erhält man die Werthe $x = 2$, $y = 15$, $z = 5$.

§. 172. *Auflösung der allgemeinsten Form der homogenen Gleichung mit drei Unbekannten.*

Dieselbe sei in der Gestalt

(1) $$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz = 0$$

gegeben, worin die Koeffizienten der in Produkte von zwei Unbekannten multiplizirten Glieder paare Zahlen seien.

Multiplizirt man diese Gleichung mit a; so lässt sich dieselbe in die Form

(2) $$(ax + dy + ez)^2 - (d^2 - ab)y^2 - 2(de - af)yz - (e^2 - ac)z^2 = 0$$

oder wenn man zur Abkürzung

(3) $$D = d^2 - ab, \quad E = de - af, \quad F = e^2 - ac$$

setzt, in die Form

(4) $$(ax + dy + ez)^2 - Dy^2 - 2Ez - Fz^2 = 0$$

bringen. Multiplizirt man jetzt mit $-D$; so entsteht leicht die Form

(5) $$-D(ax + dy + ez)^2 + (Dy + Ez)^2 - (E^2 - DF)z^2 = 0$$

oder wenn man

(6) $$X = Dy + Ez, \quad Y = ax + dy + ez, \quad Z = z$$

setzt,

(7) $$X^2 - DY^2 - (E^2 - DF)Z^2 = 0$$

Diese reduzirte Gleichung ist nach §. 161 für X, Y, Z aufzulösen. Schliesslich hat man nach den Beziehungen (6)

(8) $x = \frac{-dX + DY + (dE - eD)Z}{aD}, \quad y = \frac{X - EZ}{D}, \quad z = Z$

als Auflösung der gegebenen Gleichung.

Beispiel: $3x^2 - 7y^2 - 2z^2 + 2xy - 4xz + 8yz = 0$

Hier hat man $D = 1^2 - 3(-7) = 22$, $E = 1(-2) - 3.4 = -14$, $F = (-2)^2 - 3(-2) = 10$, $E^2 - DF = (-14)^2 - 22.10 = -24$. Die reduzirte Gleichung ist also

$$X^2 - 22Y^2 = -24Z^2$$

Um diese Gleichung nach §. 161 aufzulösen, hat man $K = \frac{\sqrt{22} + P_0}{-24}$, und es sind die durch 24 theilbaren Zahlen von der Form $22 - p^2$ zu suchen. Man findet, dass es deren nicht gibt. Nun hat aber 24 den quadratischen Faktor $4 = 2^2$. Sondert man denselben ab; so bleibt die Gleichung

$$X_1^2 - 22Y_1^2 = -6Z_1^2$$

zu behandeln. Hierfür hat man $P_0 = \pm 2$ und wenn man einmal $P_0 = 2$ nimmt, $K = \frac{\sqrt{22} + 2}{-6}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
-2					0	1
-1		-3	3		1	0
0	2	-6	-6	-1	-1	1
1	4	-1	1			

In dieser Entwickelung kann man bei $m = 1$ schliessen. Dies gibt $m = 1$, $(-1)^m Q_m = 1$, $P_m = 4$, $Q_m = -1$, $M_{m-1} = -1$, $N_{m-1} = 1$, $M_{m-2} = 1$, $N_{m-2} = 0$ und die transformirte Gleichung ist

$$x'^2 - y'^2 = 22z'^2$$

und daraus folgt nach §. 160, wenn $pq = 22$ ist,

$$x' = \frac{u}{2}(pv^2 + qw^2), \qquad y' = \frac{u}{2}(pv^2 - qw^2), \qquad z = uvw$$

Nun hat man ferner nach der Gruppe (G) in §. 161

$$\mathfrak{M}_n = \frac{x' + 4z'}{-1} = -x' - 4z', \qquad \mathfrak{N}_n = z'$$

$$M_{m+n} = -1(-x' - 4z') + 1.z' = x' + 5z'$$

$$N_{m+n} = 1(-x' - 4z') + 0.z' = -x' - 4z'$$

$$X_1 = -6(x' + 5z') - 2(-x' - 4z') = -4x' - 22z'$$

$$Y_1 = -x' - 4z', \qquad Z_1 = y'$$

Hieraus folgt

$$X = 2X_1 = -8x' - 44z', \quad Y = 2Y_1 = -2x' - 8z', \quad Z = Z_1 = y'$$

Nach den obigen Formeln (8) ist, da man $dE - eD = 1(-14) - (-2)22 = 30$ hat,

$$x = \frac{-X + 22Y + 30Z}{66} = \frac{-6x' + 5y' - 22z'}{11}$$

$$y = \frac{X + 14Z}{22} = \frac{-4x' + 7y' - 22z'}{11}$$

$$z = Z = y'$$

Substituirt man hierin für x', y', z' die aus der transformirten Gleichung gefundenen Werthe; so kommt

$$x = -\frac{u}{22}(pv^2 + 11qw^2 + 44vw)$$

$$y = -\frac{u}{22}(-3pv^2 + 11qw^2 + 44vw)$$

$$z = \frac{u}{2}(pv^2 - qw^2)$$

Nimmt man z. B. $p = 11$, $q = 2$, $v = 0$, $w = 1$, $u = -1$; so ergeben sich die Werthe $x = 1$, $y = 1$, $z = 1$.

§. 173. Spezielle Fälle der vorstehend behandelten Gleichung.

I. Fehlte in der allgemeinen Gleichung des vorhergehenden Paragraphen das Quadrat von x, wäre also $a = 0$; so würde offenbar eine Multiplikation der gegebenen Gleichung mit a unzulässig sein, weil Dies die identische Gleichung $0 = 0$ erzeugte. In diesem Falle verwechselt man x mit Einer der beiden anderen Unbekannten y oder z, deren Quadrat vorhanden ist.

Fehlten aber die Quadrate aller drei Unbekannten, wäre also $a = 0$, $b = 0$, $c = 0$; so ist es nicht nothwendig, dass die Koeffizienten der übrigen Glieder paar sind. Man habe also

(1) $$dxy + exz + fyz = 0$$

Multiplizirt man mit Einem der Koeffizienten d, e, f, welcher nicht $= 0$ ist, z. B. mit d, und addirt dann links und rechts die Grösse efz^2; so kommt

(2) $$(dx + fz)(dy + ez) = efz^2$$

oder wenn man $ef = pq$, $z = uvw$ also $efz^2 = upv^2 . upw^2$ setzt,

$$dx + fz = upv^2, \qquad dy + ez = uqw^2.$$

Hieraus ergibt sich die Auflösung

(3) $$x = \frac{uv}{d}(pv - fw), \qquad y = \frac{uw}{d}(qw - ev), \qquad z = uvw$$

Wäre in Gl. (1) e oder $f = 0$; so würde von den beiden Fak-

toren p und q, welche dann das Produkt $pq=0$ bilden müssen, der Eine $=0$ und der andere willkürlich angenommen werden können.

Beispiel: $5xy-7xz+3yz=0$

Hier ist $pq=ef=-7.3=-21$, und

$$x=\frac{uv}{5}(pv-3w),\qquad y=\frac{uw}{5}(qw+7v),\qquad z=uvw$$

So ergeben sich z. B. für $p=3$, $q=-7$, $v=2$, $w=1$, $u=5$ die Werthe $x=6$, $y=7$, $z=10$.

II. Wäre $D=0$; so würde in §. 172 die Multiplikation mit D unstatthaft sein, da Dies zu der identischen Gleichung $0=0$ führte. Man muss dann y mit z verwechseln.

Wäre aber gleichzeitig $D=0$ und auch $F=0$, sodass also auch eine Multiplikation mit F unthunlich wäre; so reduzirt sich die Gl. (4) in §. 172 auf

$$(ax+dy+ez)^2=2Eyz$$

Hätte nun E den Werth null; so reduzirte sich die vorstehende Gleichung durch Ausziehung der Quadratwurzel auf eine diphantische Gleichung

$$(5)\qquad ax+dy+ez=0$$

vom ersten Grade, welche nach dem zweiten Abschnitte aufgelös't werden kann.

Hätte aber E einen von null verschiedenen Werth; so kann man setzen

$$(6)\qquad ax+dy+ez=uvw$$

Hierdurch wird Gl. (4)

$$uv^2.uw^2=2Eyz$$

und man kann nehmen

$$2Ey=uv^2\quad\text{also}\quad y=\frac{uv^2}{2E},\quad\text{und}\quad z=uw^2$$

Hieraus und aus Gl. (6) folgt die Auflösung

$$(7)\qquad x=-\frac{u}{2aE}(dv^2+2eEw^2-2Evw),\quad y=\frac{uv^2}{2E},\quad z=uw^2$$

Dass hierin a nicht $=0$ sein kann, leuchtet ein, weil sonst die gegebene Gl. (4) nur die beiden Unbekannten y, z enthielte, also nach dem fünften Abschnitte zu behandeln wäre.

Beispiel: $x^2+4y^2+9z^2-4xy+6xz+12yz=0$

Hier ist $D=(-2)^2-1.4=0$, $F=3^2-1.9=0$, $E=-2.3-1.6=-12$, also

$$x = \frac{-u}{-24}(-2v^2 - 72w^2 + 24vw) = -\frac{u}{12}(v - 6w)^2$$

$$y = -\frac{uv^2}{24}, \qquad z = uw^2$$

So erhält man z. B. für $v = 12$, $w = 1$, $u = 1$ die Werthe $x = -3$, $y = -6$, $z = 1$.

§. 174. Besondere Auflösung einer homogenen Gleichung, in welcher Eine Unbekannte nur auf erster Potenz vorkommt.

I. Eine homogene Gleichung mit zwei oder mehr Unbekannten, welche irgend Eine Unbekannte nur auf erster Potenz enthält, kann auch folgendermaassen aufgelös't werden. Die gegebene Gleichung besitze drei Unbekannte x, y, z, und die Grösse z sei nur auf erster Potenz vorhanden. Man habe also

(1) $$ax^2 + by^2 + dxy + exz + fyz = 0$$

Setzt man hierin

$$x = uv, \qquad y = uw$$

und lös't für z auf; so kommt

(3) $$z = -\frac{u(av^2 + bw^2 + dvw)}{ev + fw}$$

Hierin kann man für v und w willkürliche ganze Zahlen setzen und dann u stets so bestimmen, dass auch z eine ganze Zahl wird.

Beispiel: $$2x^2 + 5xy - 7xz + 3yz = 0$$

Hier hat man

$$x = uv, \qquad y = uw, \qquad z = \frac{uv(2v + 5w)}{7v - 3w}$$

Nimmt man einmal $v = 2$, $w = 3$; so kommt

$$x = 2u, \qquad y = 3u, \qquad z = \frac{38u}{5}$$

also für $u = 5$

$$x = 10, \qquad y = 15, \qquad z = 38$$

II. Man kann die Auflösung der obigen Gleichung (1) auch in einer solchen Form darstellen, dass kein Nenner mehr als Eine Veränderliche enthält. Zu dem Ende schreibe man

$$ax^2 + by^2 + dxy + (ex + fy)z = 0$$

Setzt man nun

(4) $$x = uv \quad \text{und} \quad ex + fy = uw, \quad \text{also}$$

(5) $$y = \frac{u(w - v)}{f}$$

so ergibt eine Auflösung für z

(6) $$z = -\frac{u}{f^2 w}[af^2v^2 + b(w-v)^2 + dv(w-v)]$$

Homogene Gleichungen in rationalen Zahlen.

§. 175. *Auflösungsverfahren.*

Eine homogene Gleichung mit beliebig vielen Unbekannten ist stets dann, aber auch nur dann in rationalen Zahlen lösbar, wenn sie es in ganzen Zahlen ist, und umgekehrt. Denn denkt man sich alle möglichen rationalen (also auch ganzen) Werthe der Unbekannten $X, Y, Z\ldots$, welche eine Gleichung von der Form

(1) $$aX^2 + bY^2 + cXY + dXZ + \text{etc.} = 0$$

erfüllen, auf einerlei Benennung t gebracht, sodass $X = \frac{x}{t}$, $Y = \frac{y}{t}$, $Z = \frac{z}{t}$ etc. ist, und multiplizirt die gegebene quadratische Gleichung mit t^2; so entsteht die ganz gleich gebildete Gleichung

(2) $$ax^2 + by^2 + cxy + dxz + \text{etc.} = 0$$

welche nun in ganzen Zahlen $x, y, z\ldots$ lösbar sein muss.

Die allgemeinen Ausdrücke der möglichen rationalen Auflösungen der Gl. (1) erhält man also, wenn man die allgemeinen Ausdrücke der möglichen ganzen Auflösungen durch Ein und dieselbe willkürliche ganze Zahl t dividirt.

Allgemeine Gleichungen mit zwei Unbekannten in rationalen Zahlen.

§. 176. *Auflösungsverfahren.*

Wenn man eine homogene Gleichung mit drei Unbekannten in ganzen Zahlen lösen kann; so ist es leicht, eine nicht homogene oder allgemeine Gleichung mit zwei Unbekannten in rationalen Zahlen generell zu lösen. Denn verlangt man für die beiden Unbekannten X, Y der Gleichung

(1) $$aX^2 + bY^2 + 2dXY + 2eX + 2fY = k$$

nur rationale Werthe; so kann man sich dieselben auf einerlei Benennung z gebracht denken, also

(2) $$X = \frac{x}{z}, \quad Y = \frac{y}{z}$$

setzen. Hierdurch geht die gegebene Gleichung, wenn man dieselbe mit z^2 multiplizirt, über in

$$(3) \qquad ax^2 + by^2 + 2dxy + 2exz + 2fyz = kz^2$$

oder wenn man $-k = c$ setzt, in

$$(4) \qquad ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz = 0$$

Dies ist eine homogene Gleichung mit drei Unbekannten x, y, z, welche nach §. 172 in ganzen Zahlen aufzulösen ist.

Berücksichtigt man nach §. 161, VI. die allgemeine Form der Ausdrücke, in welchen sich die Werthe von x, y, z darstellen werden; so folgt für die rationalen Werthe der Unbekannten X, Y aus der gegebenen Gleichung (1) die allgemeine Form

$$(5) \qquad X = \frac{x}{z} = \frac{E_2}{E} \cdot \frac{Av^2 + Bw^2 + Cvw}{A_2v^2 + B_2w^2 + C_2vw}$$

$$(6) \qquad Y = \frac{y}{z} = \frac{E_2}{E_1} \cdot \frac{A_1v^2 + B_1w^2 + C_1vw}{A_2v^2 + B_2w^2 + C_2vw}$$

Aus diesen Ausdrücken ist die Grösse u verschwunden und v, w bleiben ganz willkürlich.

Beispiel: $\quad 3X^2 - 7Y^2 + 2XY - 4X + 8Y = 2$

Setzt man hierin $X = \frac{x}{z}$, $Y = \frac{y}{z}$; so kommt

$$3x^2 - 7y^2 - 2z^2 + 2xy - 4xz + 8yz = 0$$

Für diese Gleichung sind in §. 174 die Auflösungen

$$x = -\frac{u}{22}(pv^2 + 11qw^2 + 44vw)$$

$$y = -\frac{u}{22}(-3pv^2 + 11qw^2 + 44vw)$$

$$z = \frac{u}{2}(pv^2 - qw^2)$$

gefunden, worin $pq = 22$ ist. Hiernach hat man

$$X = \frac{x}{z} = \frac{pv^2 + 11qw^2 + 44vw}{11(-pv^2 + qw^2)}$$

$$Y = \frac{y}{z} = \frac{-3pv^2 + 11qw^2 + 44vw}{11(-pv^2 + qw^2)}$$

So hat man z. B. für $p = 11$, $q = 2$, $v = 1$, $w = 4$

$$X = \frac{7}{3}, \qquad Y = \frac{15}{7}$$

Achter Abschnitt.

Allgemeine Gleichungen vom zweiten Grade mit drei und mehr Unbekannten.

Homogene Gleichungen mit vier Unbekannten in ganzen Zahlen.

§. 177. ***Auflösung der Gleichung:***

(1) $$\alpha^2x^2 - \beta^2y^2 = cz^2 + dt^2$$

in welcher zwei Glieder die Differenz zweier Quadrate bilden.

Setzt man in dieser Gleichung

(2) $$z = uv, \qquad t = uw$$

und schreibt dieselbe in der Form

$$(\alpha x + \beta y)(\alpha x - \beta y) = u^2(cv^2 + dw^2)$$

so kann man offenbar, wenn p irgend einen Faktor der Grösse $cv^2 + dw^2$ darstellt, allgemein

(3) $$\alpha x + \beta y = up$$

(4) $$\alpha x - \beta y = \frac{u(cv^2 + dw^2)}{p}$$

setzen. Hieraus folgt

(5) $$x = \frac{u(p^2 + cv^2 + dw^2)}{2\alpha p} \text{ oder auch } = \frac{u}{2\alpha}\left(p + \frac{cv^2 + dw^2}{p}\right)$$

(6) $$y = \frac{u(p^2 - cv^2 - dw^2)}{2\beta p} \quad » \quad » \quad = \frac{u}{2\beta}\left(p - \frac{cv^2 + dw^2}{p}\right)$$

Es leuchtet ein, dass man in den Ausdrücken (5), (6), (2), welche die Auflösung der gegebenen Gleichung darstellen, für v, w, p beliebige ganze Zahlen setzen und darauf u so bestimmen kann, dass x, y, z, t ganze Zahlen werden. Man braucht nämlich für u nur einen Generalneuner der Brüche aus (5) und (6) anzunehmen. Im Übrigen erhält man meistens kleinere

Zahlen für die Unbekannten x, y, wenn man erst v und w beliebig wählt, dann für p einen Faktor der Grösse $cv^2 + dw^2$ annimmt und hierauf u so bestimmt, dass x und y ganze Zahlen werden. Auf diese Bemerkung kann man auch in den späteren ähnlichen Fällen Rücksicht nehmen.

Beispiel: $$9x^2 - 4y^2 = 2z^2 + 7t^2$$

Hier hat man

$$x = \frac{u(p^2 + 2v^2 + 7w^2)}{6p}, \quad y = \frac{u(p^2 - 2v^2 - 7w^2)}{4p}$$

$$z = uv, \qquad t = uw$$

Setzt man z. B. $v = 1$, $w = 1$, $p = 4$; so kommt

$$x = \frac{25u}{24}, \quad y = \frac{7u}{16}, \quad z = u, \quad t = u$$

also für $u = 48$

$$x = 50, \quad y = 21, \quad z = 48, \quad t = 48$$

Setzt man $v = 1$, $w = 1$ und nimmt für p einen Faktor von $2v^2 + 7w^2 = 9$, etwa den Werth $p = 3$; so kann man $u = 1$ setzen und erhält

$$x = 1, \quad y = 0, \quad z = 1, \quad t = 1$$

§. 178. Behandlung der Gleichung:

$$ax^2 + by^2 + cz^2 + dt^2 = 0$$

I. Wenn alle Koeffizienten dieser Gleichung einerlei Zeichen hätten; so würde offenbar ausser der Auflösung $x = y = z = t = 0$ keine andere möglich sein.

Schliessen wir also diesen Fall aus; so müssen irgend zwei Koeffizienten entgegengesetzte Zeichen haben. Angenommen, Dies seien die beiden a und b. Wir wollen nun die fragliche Gleichung als in der Form

(1) $$ax^2 - by^2 = cz^2 + dt^2$$

gegeben ansehen, worin a und b positiv sind, c und d aber beliebige Zeichen haben können.

Jetzt kommt es uns darauf an, zu bewirken, dass das erste Glied auf der linken Seite ein vollkommenes Quadrat werde, und zugleich, dass das erste Glied auf der rechten Seite entweder ebenfalls ein vollkommenes Quadrat werde, oder doch neben einem quadratischen Faktor nur noch einen solchen nicht quadratischen Faktor besitze, welcher auch dem zweiten Gliede auf der rechten Seite gemein ist. Wäre dieser Zustand nicht schon in der gegebenen Gleichung erfüllt; so erreichen wir denselben, indem wir dieselbe mit ac^2 multipliziren und

alsdann durch Absonderung des gemeinschaftlichen Faktors ac auf der rechten Seite

(2) $$(acx)^2 - abc^2y^2 = ac[(cz)^2 + cdt^2]$$

schreiben.

Um möglichst kleine Zahlen zu erhalten, braucht man, wenn a oder c quadratische Faktoren enthalten, wenn also $a=\alpha^2a'$ und $c=\gamma^2c'$ ist, nicht mit ac^2, sondern nur mit $a'c'^2$ zu multipliziren. Ferner braucht man, wenn die nicht quadratischen Faktoren a' und c' von a und c ein gemeinschaftliches Maass μ besitzen sollten, wenn also $a'=A\mu$ und $c'=C\mu$ sein sollte, auch nicht mit $a'c'^2$, sondern nur mit $AC^2\mu$ zu multipliziren. In dem letzteren allgemeineren Falle, wo also

$$a=\alpha^2A\mu, \qquad c=\gamma^2C\mu$$

ist, erhält man durch Multiplikation mit $AC^2\mu$

(2*) $$(\alpha AC\mu x)^2 - AC^2b\mu y^2 = AC[(\gamma C\mu z)^2 + C\mu dt^2]$$

Hierin kann nun der Faktor AC auf der rechten Seite, da A und C weder quadratische Faktoren, noch ein gemeinschaftliches Maass besitzen, keinen quadratischen Faktor enthalten. Der einfacheren Schreibweise wegen wollen wir jedoch bei der Form der Gl. (2) stehen bleiben. Es wird leicht sein, in jedem speziellen Falle, wo die zuletzt erwähnte Vereinfachung thunlich ist, dieselbe in Anwendung zu bringen, und die dadurch sich erzeugenden Koeffizienten nach den folgenden Prinzipien weiter zu behandeln.

II. Wenn wir jetzt nach den Prinzipien des §. 161 die Grössen acx und y der Gl. (2) wie die beiden Veränderlichen auf der linken Seite behandeln, und

(3) $$D=abc^2, \quad Q_0=ac, \quad (-1)^{m+n+1}Q_{m+n+1}=(cz)^2+cdt^2$$

annehmen, also uns die Kettenbruchsentwickelung

(4) $$K=\frac{\sqrt{D}+P_0}{Q_0}=\frac{\sqrt{abc^2}+P_0}{ac}$$

vergegenwärtigen; so erhellet, dass wenn die gegebene Gleichung überhaupt lösbar sein soll, es Zahlen von der Form $abc^2-P_0^2$ geben muss, welche durch ac theilbar sind. Derartige Zahlen sind offenbar stets vorhanden. Denn zunächst bietet sich hier immer der Werth $P_0=0$ dar. Dies ist sogar, wenn $Q_0=ac$ keinen quadratischen Faktor besitzt, der einzig zulässige Werth für P_0. Denn alsdann muss die Grösse ac, da sie in abc^2 aufgeht, also auch in P_0^2 aufgehen muss, auch in P_0 enthalten sein. Es kann also P_0 nur ein Vielfaches von ac sein, und Dies entspricht, da ja nur die Werthe von P_0, welche $\leqq\frac{ac}{2}$ sind, in Betracht kommen, dem einzigen Werthe $P_0=0$. Be-

sässe jedoch $Q_0 = ac$ einen quadratischen Faktor, den man übrigens nach der obigen Rechnung stets vermeiden kann; so wären allerdings ausser dem Werthe $P_0 = 0$ unter Umständen auch noch andere Werthe von P_0 denkbar.

Jetzt assimiliren wir die Gl. (2) in ähnlicher Weise, wie Dies in §. 161 geschehen ist, der Gleichung

(5) $(Q_0 M_{m+n} - P_0 N_{m+n})^2 - D N_{m+n}^2 = (-1)^0 Q_0 (-1)^{m+n+1} Q_{m+n+1}$

indem wir neben den in Gl. (3) und (4) angegebenen Vergleichungen

(6) $acx = Q_0 M_{m+n} - P_0 N_{m+n}, \qquad y = N_{m+n}$

setzen.

Nachdem alsdann die vorhin beschriebenen Werthe von P_0 ermittelt sind und für irgend Einen derselben die Grösse K aus Gl. (4) in einen Kettenbruch entwickelt ist, gehen wir zu der bekannten Gleichung

(7) $(Q_m \mathfrak{M}_n - P_m \mathfrak{N}_n)^2 - D \mathfrak{N}_n^2 = (-1)^m Q_m (-1)^{m+n+1} Q_{m+n+1}$

über. Findet sich in der Entwickelung von K unter den Grössen $(-1)^m Q_m$ ein vollkommenes Quadrat; so nehmen wir dasselbe in der vorstehenden Gleichung für $(-1)^m Q_m$, und sind damit zur Schlussgleichung gelangt. Ist aber unter jenen Grössen kein Quadrat vorhanden; so beachte man, dass wegen $P_0 = 0$ die Grösse $Q_{-1} = \frac{D - P_0^2}{Q_0} = \frac{abc^2}{ac} = bc$ ist. Es wird also, gleichviel, ob schon die Periode der Grössen Q mit dem Zeiger -1 oder erst später beginnt, in dieser Periode jedenfalls ein Werth angetroffen werden, welcher numerisch $\leqq Q_{-1}$ d. i. $\leqq bc$ ist. Für irgend eine aus der Periode jener Grössen genommene Zahl sei

(8) $(-1)^m Q^m = q$

Setzt man diesen einfacheren Ausdruck für $(-1)^m Q_m$ in Gl. (7); so wird dieselbe, indem man zur ferneren Abkürzung

(9) $x' = Q_m \mathfrak{M}_n - P_m \mathfrak{N}_n, \qquad y' = \mathfrak{N}_n$

setzt, unter Berücksichtigung der Werthe von D und $(-1)^{m+n+1} Q_{m+n+1}$ aus Gl. (3)

(10) $x'^2 - abc^2 y'^2 = q[(cz)^2 + cdt^2)]$

und stellt die erste transformirte Gleichung dar.

III. Jetzt lassen wir auf der linken und rechten Seite die ersten Glieder stehen und transponiren die zweiten. Dies gibt

$$-cdqt^2 + x'^2 = q(cz)^2 + abc^2 y'^2$$

Mit dieser Gleichung verfahren wir wie mit der gegebenen, unter Beachtung der obigen Bemerkung hinsichtlich der Erzielung möglichst kleiner Zahlen, multipliziren also mit $-cdq$ und erhalten

(11) $$(cdqt)^2-cdqx'^2=-cd[(cqz)^2+abc^2qy'^2]$$

Diese Gleichung ist wie Gl. (2) zu behandeln; es ist also

(12) $D'=cdq,\quad Q_0'=-cd,\quad (-1)^{m'+n'+1}Q'_{m'+n'+1}=(cqz)^2+Dqy'^2$

(13) $$cdqt=Q_0'M'_{m'+n'}-P_0'N'_{m'+n'},\qquad x'=N_{m'+n'}$$

zu nehmen und

(15) $$K'=\frac{\sqrt{D'}+P_0'}{Q_0'}=\frac{\sqrt{cdq}+P_0'}{-cd}$$

zu entwickeln, indem man die Reihen der durch cd theilbaren Zahlen von der Form $cdq-P_0'^2$ aufsucht, für welche $P_0'=0$ stets ein zulässiger und sogar dann der einzige Werth ist, wenn man dafür gesorgt hat, dass cdq keinen quadratischen Faktor enthält. Findet sich unter den Grössen $(-1)^{m'}Q'_{m'}$ ein vollkommenes Quadrat; so gibt der Übergang von Gl. (11) zu der nach (7) gebildeten Gleichung die Schlussgleichung. Findet sich jedoch nicht sofort ein solches Quadrat; so sei für irgend Eine aus der Periode der fraglichen Grössen genommene Zahl

(15) $$(-1)^{m'}Q'_{m'}=q'$$

Da $Q_{-1}'=\frac{D'-P_0'^2}{Q_0'}=\frac{cdq}{-cd}=-q$ ist; so folgt entschieden, dass der numerische Werth von $q'\leqq q$ sei. Hierdurch erhält man aus Gl. (11), indem man

(16) $$x''=Q'_{m'}\mathfrak{M}'_{n'}-P'_{m'}\mathfrak{N}'_{n'},\qquad y''=\mathfrak{N}'_{n'}$$

setzt,

(17) $$x''^2-cdqy''^2=q'[(cqz)^2+abc^2qy'^2]$$

und dies ist die zweite transformirte Gleichung.

IV. Wir transponiren nun wieder wie bei Gl. (10), was

$$-abc^2qq'y'^2+x''^2=q'(cqz)^2+cdqy''^2$$

gibt, und multipliziren mit $-abqq'$, wodurch sich

(18) $$(abcqq'y')^2-abqq'x''^2=-abq[(cqq'z)^2+cdqq'y''^2]$$

ergibt. Hiermit verfahren wir ferner wie mit Gl. (2), setzen also

(19) $$D''=abqq',\qquad Q_0''=-abq,$$

$$(-1)^{m''+n''+1}Q''_{m''+n''+1}=(cqq'z)^2+cdqq'y''^2$$

(20) $abcqq'y'=Q_0''M''_{m''+n''}-P_0''N''_{m''+n''},\qquad x''=N''_{m''+n''}$

und entwickeln

(21) $$K''=\frac{\sqrt{D''}+P_0''}{Q_0''}=\frac{\sqrt{abqq'}+P_0''}{-abq}$$

wofür stets $P_0''=0$ genommen werden kann. Findet sich unter den Grössen $(-1)^{m''}Q''_{m''}$ ein Quadrat; so liefert der Übergang von Gl. (18) zu der nach Gl. (7) gebildeten Gleichung die

Schlussgleichung. Im entgegengesetzten Falle sei für irgend Eine der periodischen Grösse dieser Art

(22) $$(-1)^{m''}Q'_{m''}=q''$$

Da $Q_{-1}''=\frac{D'-P_0''^2}{Q_0''}=\frac{abqq'}{-abq}=-q'$ ist; so folgt, dass der numerische Werth von $q''\leqq q'$ sei. Hierdurch erhält man aus Gl. (20), indem man

(23) $$x'''=Q'_{m''}\mathfrak{M}''_{n''}-P''_{m''}\mathfrak{N}''_{n''},\qquad y''=\mathfrak{N}''_{n''}$$

setzt,

(24) $$x'''^2-abqq'y'''^2=q''[(cqq'z)^2+cdqq'y''^2]$$

worin die dritte transformirte Gleichung besteht.

V. Durch die mehrerwähnte Transposition und Multiplikation mit $-cdqq'q''$ wird diese Gleichung

(25) $$(cdqq'q''y'')^2-cdqq'q''x'''^2=-cdqq'[(cqq'q''z)^2+abqq'q''y'''^2]$$

und dieselbe geht durch Entwickelung von

(26) $$K'''=\frac{\sqrt{D''}+P_0'''}{Q_0'''}=\frac{\sqrt{cdqq'q''}+P_0'''}{-cdqq'}$$

worin stets $P_0'''=0$ genommen werden kann, über in die vierte transformirte Gleichung

(27) $$x''''^2-cdqq'q''y''''^2=q'''[(cqq'q''z)^2+abqq'q''y'''^2]$$

welches die Schlussgleichung sein wird, wenn sich für q''' ein Quadrat vorfindet.

VI. Jetzt wird der Gang der Rechnung hinlänglich klar geworden sein, und es stellt sich folgendes Gesetz heraus

$D=abc^2,$	$Q_0=ac,$	$Q_{-1}=bc$
$D'=cdq,$	$Q_0'=-cd,$	$Q_{-1}'=-q$
$D''=abqq',$	$Q_0''=-abq,$	$Q_{-1}''=-q'$
$D'''=cdqq'q'',$	$Q_0'''=-bdqq',$	$Q_{-1}'''=-q''$
$D''''=abqq'q''q''',$	$Q_0''''=-abqq'q'',$	$Q_{-1}''''=-q'''$
etc.	etc.	etc.

Was die Grössen $q, q', q''\ldots$ betrifft, unter welchen wir ein Quadrat suchen; so leuchtet ein, dass wenn man auf das Zeichen derselben keine Rücksicht nimmt, und stets die numerisch kleinste aus der betreffenden Periode der Grössen $(-1)^mQ_m$, $(-1)^{m'}Q'_{m'}$, $(-1)^{m''}Q'_{m''}\ldots$ auswählt, dem numerischen Werthe nach

$$q\leqq bc,\quad q'\leqq q,\quad q''\leqq q',\quad q'''\leqq q''\ \text{etc.}$$

sein wird. Unter diesen Umständen ist jedoch nicht wie in §. 161 der Schluss gerechtfertigt, dass man endlich nothwendig auf eine Grösse q stossen müsse, welche $=\pm 1$ sei. Vielmehr kann es sich ereignen, dass von einer gewissen Stelle an, alle

folgenden Grössen dieser Art Ein und denselben numerischen Werth behalten, sodass man also durch die absoluten Minima von q nicht unbedingt die Lösung der Aufgabe erwarten kann.

Erspriesslicher für die fragliche Auflösung ist es im Allgemeinen, wenn man aus den mehr erwähnten Perioden der einzelnen Kettenbruchsentwickelungen nicht das absolute, sondern von dem positiven und negativen Minimum immer dasjenige nimmt, durch welches die zunächst folgende Determinante einen positiven Werth erhält. Um Dies zu erreichen, hat man zu nehmen, da nach der Voraussetzung ab positiv sein soll

1) wenn cd positiv ist, für jedes q das positive Minimum,
2) wenn cd negativ ist, für jedes q das negative Minimum.

Unter solchen Umständen kann man übrigens nicht behaupten, dass die Grössen $q, q', q'' \ldots$ eine abnehmende Reihe bilden und nothwendig endlich zu einem Quadrate > 1 oder zu dem Werthe $+1$ führen müssen. Das Problem ist also durch vorstehendes Verfahren nicht mit apodiktischer Gewissheit gelös't; gleichwol findet man dadurch in vielen Fällen die allgemeinen Auflösungen der gegebenen Gleichung, und es scheint demnach, als ob dieses Verfahren durch eine zweckdienliche Modifikation zur sicheren Lösung der gegebenen Gleichung in allen Fällen geschickt gemacht werden könne.

VII. Nehmen wir nun an, irgend Eine der Grössen $q, q', q'' \ldots$ sei ein vollkommenes, also auch positives Quadrat; so ist die betreffende transformirte Gleichung die Schlussgleichung. Wäre z. B.

(28) $$q = (-1)^m Q_m = x^2$$

so wäre die erste transformirte Gleichung, also Gl. (10) die Schlussgleichung. Dieselbe nimmt alsdann die Form

$$x'^2 - abc^2y'^2 = (cxz)^2 + cdx^2t^2$$

an, und wenn man das erste Glied der rechten Seite und das zweite Glied der linken Seite transponirt,

(29) $$x'^2 - (cxz)^2 = abc^2y'^2 - cdx^2t^2$$

Diese Schlussgleichung ist nach §. 177 für x', z, y', t aufzulösen. Eine rückgängige Substitution dieser Werthe in die vorhergehenden Hülfsgleichungen liefert zuvörderst aus den Beziehungen (9) die Werthe für $\mathfrak{M}_n$ und $\mathfrak{N}_n$, nämlich

(30) $$\mathfrak{M}_n = \frac{x' + P_m y'}{Q_m}, \qquad \mathfrak{N}_n = y'$$

dann vermittelst der Beziehungen (7) aus §. 161 die Werthe für M_{m+n} und N_{m+n}, nämlich

(31) $$M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n, \qquad N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n$$

und hierauf vermittelst der obigen Beziehungen (6) die Werthe für x und y.

VIII. Auch hier muss, wie in §. 161, darauf aufmerksam gemacht werden, dass wenn sich auf der rechten Seite der gegebenen oder irgend einer transformirten Gleichung ein konstanter quadratischer Faktor absondern lässt, Dies behuf allgemeiner Auflösung der Gleichung, so oft es thunlich ist, geschehen muss, indem man nach den für diesen Fall in §. 161 gegebenen Prinzipien verfährt.

IX. Es ist von Wichtigkeit, dass wenn die Gleichung $ax^2-by^2=cz^2$ lösbar ist, es auch stets die Gleichung $ax^2-by^2=cz^2+dt^2$ sein wird, welchen Werth auch d haben möge. Dies leuchtet schon daraus ein, dass man in der letzteren Gleichung für x, y, z nur die Werthe aus der ersteren und ausserdem $t=0$ zu nehmen braucht. Es lassen sich aber in diesem Falle auch diejenigen Auflösungen der letzteren Gleichung angeben, für welche t nicht $=0$ ist. Denn wenn die erstere Gleichung möglich ist; so ist es offenbar auch die Gleichung

$$(32)\qquad (acx)^2-abc^2y^2=ac(cz)^2$$

Assimilirt man diese Gleichung der Beziehung (7); so leuchtet aus §. 161, VIII. ein, dass man für $(-1)^m Q_m$ nach der dort beschriebenen Methode ein vollkommenes Quadrat finden könne. Nimmt man Dieses für q in der ersten transformirten Gleichung (10); so kann die Auflösung nach den vorstehenden Regeln erfolgen.

In dem Falle also, wo die Gleichung $ax^2+by^2+cz^2+dt^2=0$ von der Art ist, dass irgend drei Glieder derselben eine lösbare Gleichung mit drei Unbekannten bilden, kann dieselbe jederzeit allgemein aufgelös't werden.

Um zur Auflösung zu gelangen, kann man entweder erst die vorstehende dreigliederige Gleichung (32) nach §. 161 auflösen, um nach §. 161, VIII. einen quadratischen Werth für $(-1)^m Q_m$ zu ermitteln, welcher, wenn er für q gesetzt wird, sofort die erste transformirte Gl. (10) zur Schlussgleichung macht, oder man kann auch mit der gegebenen Gleichung (2), resp. (2^a), solche Transformationen vornehmen, welche den in §. 161 vorkommenden ähnlich sind und die Lösung der Gl. (32) mit enthalten.

Nach diesem letzteren Verfahren würde man auf der linken Seite stets das erste und auf der rechten Seite stets das zweite Glied unverrückt stehen lassen und nur das zweite Glied der linken und das erste Glied der rechten Seite bei dem Übergange von der Einen transformirten Gleichung zu der nächstfolgenden transponiren. Es ist jedoch hierbei auch noch der von der Multiplikation mit c^2 herrührende quadratische Faktor

des Koeffizienten des zweiten Gliedes links mit der unbekannten Grösse selbst zu vereinigen, also statt Gl. (2) zu schreiben

(33) $$(acx)^2-ab(cy)^2=ac[(cz)^2+cdt^2]$$

Die Entwickelung von $K=\frac{\sqrt{ab}+P_0}{ac}$ führt jetzt zu der ersten transformirten Gleichung

(34) $$x'^2-aby'^2=q[(cz)^2+cdt^2]$$

oder

(35) $$x'^2-q(cz)^2=aby'^2+cdqt^2$$

Multiplizirt man mit $(ab)^2$; so kommt

(36) $$(abx')^2-q(abcz)^2=ab[(aby')^2+abcdqt^2]$$

und wenn man $K'=\frac{\sqrt{q}+P_0'}{ab}$ entwickelt; so ergibt sich die zweite transformirte Gleichung

(37) $$x''^2-qy''^2=q'[(aby')^2+abcdqt^2]$$

oder

(38) $$x''^2-q'(aby')^2=q(y''^2+abcdq't^2)$$

Jetzt ist eine Multiplikation nicht weiter erforderlich. Durch Entwickelung von $K''=\frac{\sqrt{q'}+P_0''}{q}$ ergibt sich die dritte transformirte Gleichung

(39) $$x'''^2-q'y'''^2=q''(y''^2+abcdq't^2)$$

oder

(40) $$x'''^2-q''y''^2=q'(y'''^2+abbdq''t^2)$$

Hieraus ergibt sich durch Entwickelung von $K'''=\frac{\sqrt{q''}+P_0'''}{q'}$ die vierte transformirte Gleichung u. s. f.

Die Bedingung, unter welcher dieses Verfahren zur Auflösung führt, besteht in der Lösbarkeit der Gleichung (32), also in der Möglichkeit der Entwickelungen von K, K', K'' ...

X. Da das sub I. bis VIII. beschriebene Verfahren nicht in allen Fällen unbedingt zum Ziele führt, und auch das sub IX. gelehrte nicht immer anwendbar ist; so ist es von Interesse, noch fernere Modifikationen zu bezeichnen, welche zuweilen dann die Lösung herbeiführen, wenn Dies mit jenen beiden Methoden nicht gelingt. Zu diesem Ende dürfte noch folgendes Verfahren zu beachten sein.

Aus der gegebenen Gl. (1) werde die Gl. (2) oder (2ª) hergestellt, welche wir kurz

(41) $$X^2-DY^2=Q_0(Z^2-ET^2)$$

schreiben wollen. Hieraus folgt durch Entwickelung der Grösse $K=\frac{\sqrt{D}+P_0}{Q_0}$ in einen Kettenbruch die erste transformirte Gleichung (10), also

(42) $$X'^2-DY'^2=q(Z^2-ET^2)$$

Diese Gleichung wird, wenn q kein Quadrat ist, durch Multiplikation mit q

$$q(X'^2-DY'^2)=(qZ)^2-E(qT)^2=Z'^2-ET'^2$$

oder wenn man dieselbe umkehrt,

(43) $$Z'^2-ET'^2=q(X'^2-DY'^2)$$

Jetzt ist $K'=\frac{\sqrt{E}+P_0'}{q}$ in einen Kettenbruch zu entwickeln. **Hierdurch ergibt sich als zweite transformirte Gleichung**

(44) $$q'(X'^2-DY'^2)=Z''^2-ET''^2$$

Ist q' kein Quadrat; so multiplizirt man damit. Dies gibt

(45) $(q'X')^2-D(q'Y')^2$ oder $X''^2-DY''^2=q'(Z''^2-ET''^2)$

Jetzt ist $K''=\frac{\sqrt{D}+P_0''}{q'}$ zu entwickeln. Hierdurch gelangt man zu der dritten transformirten Gleichung

(46) $$X'''^2-DY'''^2=q''(Z''^2-ET''^2)$$

welche, wenn q'' kein Quadrat ist, durch Multiplikation mit q'' in

$$q''(X'''^2-DY'''^2)=(q''Z'')^2-E(q''T'')^2=Z'''^2-ET'''^2$$

oder durch Umkehrung in

(47) $$Z'''^2-ET'''^2=q''(X'''^2-DY'''^2)$$

übergeht und wie die Gl. (34) zu behandeln ist, indem man jetzt $K'''=\frac{\sqrt{E}+P_0'''}{q''}$ entwickelt.

Sobald man für q, q', q'' oder eine spätere dieser Grössen ein Quadrat findet, kann man die Rechnung schliessen, indem sich dann die Schlussgleichung nach §. 177 lösen und durch rückgängige Substitution die Lösung der gegebenen Gleichung darstellen lässt.

XI. Wenn zwei Glieder der gegebenen Gleichung einen gemeinschaftlichen Faktor besitzen, wenn also eine Gleichung von der Form

(48) $$ax^2-by^2=k(cz^2+dt^2)$$

gegeben wäre; so erfordert die Lösbarkeit vor allen Dingen, dass es ganze Zahlen von der Form $\frac{ab-P_0^2}{k}$ gebe. Es gereicht oftmals zur Vereinfachung der Rechnung, wenn man

einen solchen den Gliedern auf der rechten Seite gemeinschaftlichen Faktor k gleich von vorn herein absondert. Derselbe bildet dann sogleich einen Faktor der in Gl. (2), resp. (2[a]) auf der rechten Seite vor der Klammer stehenden Grösse ac, resp. AC, mit welchem man die ganze Gleichung nicht weiter zu multipliziren braucht.

§. 179. **Beispiel:**

$$5x^2-7y^2+2z^2-3t^2=0$$

Transponiren wir die letzten beiden Glieder; so kommt

$$5x^2-7y^2=-2z^2+3t^2$$

und wenn man nun mit $5.2^2=20$ multiplizirt,

$$(10x)^2-140y^2=-10[(2z)^2-6t^2]$$

Diese Gleichung tritt an die Stelle der Gl. (2) in §. 178. Wir haben also $D=140$, $Q_0=-10$, $K=\frac{\sqrt{140}+P_0}{-10}$. Da Q_0 keinen quadratischen Faktor hat; so kann nur $P_0=0$ sein. Dies gibt $K=\frac{\sqrt{140}+0}{-10}$

m	P_m	Q_m	$(-1)_m Q_m$	a_m	M_m	N_m
-2					0	1
-1		-14	14		1	0
0	0	-10	-10	-2	-2	1
1	20	26	-26	1	-1	1
2	6	4	4			

Da man schon in dieser Entwickelung bei $(-1)^2Q_2=4$ auf ein Quadrat stösst; so kann man die Rechnung schliessen, indem man setzt $m=2$, $P_m=6$, $Q_m=4$, $(-1)^mQ_m=q=4$, $M_{m-1}=-1$, $N_{m-1}=1$, $M_{m-2}=-2$, $N_{m-2}=1$. Die Schlussgleichung, welche die Stelle von Gl. (10) in §. 178 vertritt, ist

$$x'^2-140y'^2=4[(2z)^2-6t^2]$$

Dieselbe gibt durch Transposition

$$x'^2-(4z)^2=140y'^2-24t^2$$

Die Auflösung dieser Gleichung nach §. 177 ist

$$x'=\frac{u}{2p}(p^2+140v^2-24w^2), \qquad z=\frac{u}{8p}(p^2-140v^2+24w^2)$$

$$y'=uv, \qquad t=uw$$

Durch die rückgängige Substitution erhält man

$$\mathfrak{M}_n=\frac{x'+P_my'}{Q_m}=\frac{x'+6y'}{4}, \qquad \mathfrak{N}_n=y'$$

$$M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n = (-1).\frac{x'+6y'}{4} + (-2)y' = -\frac{x'+14y'}{4}$$

$$N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n = 1.\frac{x'+6y'}{4} + 1.y' = \frac{x'+10y'}{4}$$

$$10x = Q_0 M_{m+n} - P_0 N_{m+n} = -10\left(-\frac{x'+14y'}{4}\right) - 0.\frac{x'+10y'}{4}$$

$$x = \frac{x'+14y'}{4}$$

$$y = N_{m+n} = \frac{x'+10y'}{4}$$

Substituirt man in diese Werthe von x und y die für x' und y' aus der Schlussgleichung gefundenen Ausdrücke, und schreibt daneben die aus der letzteren Gleichung auch für z und t erhaltenen Werthe; so ist die Auflösung der gegebenen Gleichung dargestellt durch

$$x = \frac{u}{8p}[p^2 + 4(35v^2 - 6w^2 + 7pv)]$$

$$y = \frac{u}{8p}[p^2 + 4(35v^2 - 6w^2 + 5pv)]$$

$$z = \frac{u}{8p}[p^2 - 4(35v^2 - 6w^2)]$$

$$t = uw$$

So hat man z. B. für $v=1$, $w=1$, $p=2$, $u=1$ die Werthe $x=11$, $y=10$, $z=-7$, $t=1$.

§. 180. Beispiel:

$$x^2 + y^2 + z^2 = 770t^2$$

Schreiben wir

$$x^2 - 770t^2 = -1(y^2 + z^2)$$

so ist sofort $D=770$, $Q_0=-1$, $K=\frac{\sqrt{770}+0}{-1}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
−2					0	1
−1		−770	770		1	0
0	0	−1	−1	−28	−28	1
1	28	14	−14	3	−83	3
2	14	41	41	1		
3	27	1	−1	54		
4	27	41	41	1		
5	14	14	−14	2		
6	14	41	41	1		

In dieser Entwickelung kommt unter den Grössen $(-1)^m Q_m$ kein Quadrat vor. Nehmen wir den kleinsten darunter vorkommenden positiven Werth 41; so können wir setzen $m = 2$, $P_m = 14$, $Q_m = 41$, $(-1)^m Q_m = q = 41$, $M_{m-1} = -83$, $N_{m-1} = 3$, $M_{m-2} = -28$, $N_{m-2} = 1$.

Hieraus folgt die erste transformirte Gleichung

$$x'^2 - 770y'^2 = 41(y^2 + z^2)$$

oder durch Transposition

$$41z^2 - x'^2 = -41y^2 - 770y'^2$$

und wenn man nun mit 41 multiplizirt,

$$(41z)^2 - 41x'^2 = -1[(41y)^2 + 41\,.\,770y'^2]$$

Jetzt haben wir $D' = 41$, $Q_0' = -1$, $K' = \frac{\sqrt{41} + 0}{-1}$

m'	$P'_{m'}$	$Q'_{m'}$	$(-1)^{m'}Q'_{m'}$	$a_{m'}$	$M'_{m'}$	$N'_{m'}$
−2					0	1
−1		−41	41		1	0
0	0	−1	−1	−7	−7	1
1	7	8	−8	1	−6	1
2	1	5	5	1	−13	2
3	4	5	−5	2	−32	5
4	6	1	1			

Diese Entwickelung führt zum Schlusse; man kann setzen $m' = 4$, $P'_{m'} = 6$, $Q'_{m'} = 1$, $(-1)^{m'}Q'_{m'} = q' = 1$, $M'_{m'-1} = -32$, $N'_{m'-1} = 5$, $M'_{m'-2} = -13$, $N'_{m'-2} = 2$. Die Schlussgleichung ist also

$$x''^2 - 41y''^2 = 1[(41y)^2 + 41\,.\,770y'^2]$$

oder durch Transposition

$$x''^2 - (41y)^2 = 41y''^2 + 41\,.\,770y'^2$$

Diese Gleichung kann nach §. 177 aufgelös't werden und ergibt

$$x'' = \frac{u}{2p}[p^2 + 41(v^2 + 770w^2)], \quad y = \frac{u}{82p}[p^2 - 41(v^2 + 770w^2)]$$

$$y'' = uv, \qquad y' = uw$$

Die rückgängige Substitution liefert

$$\mathfrak{M}'_{n'} = \frac{x'' + P'_{m'}y''}{Q'_{m'}} = x'' + 6y'', \qquad \mathfrak{N}'_{n'} = y''$$

$$M'_{m'+n'} = M'_{m'-1}\mathfrak{M}'_{n'} + M'_{m'-2}\mathfrak{N}'_{n'} = -(32x'' + 205y'')$$

$$N'_{m'+n'} = N'_{m'-1}\mathfrak{M}'_{n'} + N'_{m'-2}\mathfrak{N}'_{n'} = 5x'' + 32y''$$

$$41z = Q_0'M'_{m'+n'} - P_0'N'_{m'+n'} = 32x'' + 205y''$$

$$z = \frac{32x'' + 205y''}{41}$$

$$x' = N'_{m'+n'} = 5x'' + 32y''$$

$$\mathfrak{M}_n = \frac{x' + P_m y'}{Q_m} = \frac{5x'' + 32y'' + 14y'}{41}, \qquad \mathfrak{N}_n = y'$$

$$M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n = -\frac{83(5x'' + 32y'') + 14.85y'}{41}$$

$$N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n = \frac{3(5x'' + 32y'') + 43y'}{41}$$

$$x = Q_0 M_{m+n} - P_0 N_{m+n} = \frac{83(5x'' + 32y'') + 14.85y'}{41}$$

$$t = N_{m+n} = \frac{3(5x'' + 32y'') + 43y'}{41}$$

Substituirt man in die vorstehenden Ausdrücke für x, z und t die aus der Schlussgleichung für x'', y'', y' gefundenen Werthe und notirt daneben auch den aus der Schlussgleichung hervorgegangenen Werth von y; so stellt sich die Auflösung der gegebenen Gleichung in folgenden Formeln dar.

$$x = -\frac{u}{82p}[5.83(p^2 + 41v^2 + 41.770w^2) + 64.83pv + 28.85pw]$$

$$y = \frac{u}{82p}(p^2 - 41v^2 - 41.770w^2)$$

$$z = \frac{u}{41p}[16(p^2 + 41v^2 + 41.770w^2) + 5.41pv]$$

$$t = \frac{u}{82p}[15(p^2 + 41v^2 + 41.770w^2) + 6.32pv + 86pw]$$

Nimmt man einmal $v=0$, $w=0$, $p=1$, $u=82$; so kommt

$$x = -415, \quad y = 1, \quad z = 32, \quad t = 15$$

worin x auch positiv genommen werden kann.

§. 181. **Beispiel:**

$$x^2 = 528y^2 - 618z^2 + 1854t^2$$

Da die Gleichung $x^2 = 528y^2 - 618z^2$, welche wir in §. 165 behandelt haben, lösbar ist; so muss es nothwendig auch die vorstehende sein.

Bringen wir demnach das Verfahren §. 178, IX. in Anwendung, indem wir nach §. 178, XI. beachten, dass sich die gegebene Gleichung in die Form

$$x^2 - 528y^2 = -618(z^2 + 3t^2)$$

stellen lässt; so haben wir $D=528$, $Q_0=-618$, $K=\frac{\sqrt{528}+P_0}{-618}$. Hierin kann nach §. 165 unter Anderem $P_0=42$, also

$K\frac{\sqrt{528}+42}{-618}$ genommen werden. Um in der Entwickelung dieses Werthes von K unter den Grössen $(-1)^m Q_m$ ein Quadrat zu erlangen, kann man, wie schon in §. 165 gezeigt ist, $K=[0, -19]$ nehmen. Dies gibt $m=2$, $P_m=4$, $Q_m=256$, $(-1)^m Q_m = q = 256 = 16^2$, $M_{m-1}=1$, $N_{m-1}=-19$, $M_{m-2}=0$, $N_{m-2}=1$ und die erste transformirte Gleichung, welche auch die Schlussgleichung ist, wird

$$x'^2 - 528y'^2 = 256(z^2+3t^2) \quad \text{oder}$$
$$x'^2 - (16z)^2 = 528y'^2 + 768t^2$$

Hieraus folgt nach §. 177

$$x' = \frac{u}{2p}(p^2+528v^2+768w^2), \qquad z = \frac{u}{32p}(p^2-528v^2-768w^2)$$
$$y' = uv, \qquad t = uw$$

Die rückgängigen Substitutionen liefern

$$\mathfrak{M}_n = \frac{x'+P_m y'}{Q_m} = \frac{x'+4y'}{256}, \qquad \mathfrak{N}_n = y'$$

$$M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n = \frac{x'+4y'}{256}$$

$$N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n = \frac{-19x'+180y'}{256}$$

$$x = Q_0 M_{m+n} - P_0 N_{m+n} = \frac{45x' - 2508y'}{64}$$

$$y = N_{m+n} = \frac{-19x'+180y'}{256}$$

Führt man in diese Werthe von x und y die obigen Werthe von x' und y' ein, und notirt daneben auch die obigen Werthe von z und t; so ergibt sich folgende Auflösung der gegebenen Gleichung.

$$x = \frac{3u}{128p}[15(p^2+528v^2+768w^2) - 1672pv]$$

$$y = \frac{u}{512p}[-19(p^2+528v^2+768w^2)+360pv]$$

$$z = \frac{u}{32p}(p^2-528v^2-768w^2)$$

$$t = uw$$

Nimmt man einmal $v=0$, $w=1$, $p=2$, $u=256$; so kommt $x=34740$, $y=-3667$, $z=-3056$, $t=256$.

§. 182. **Beispiel:**

$$x^2 + z^2 = 3y^2 + 7t^2$$

Schreiben wir diese Gleichung in der Form

$$x^2 - 3y^2 = -1(z^2 - 7t^2)$$

und behandeln wir dieselbe nach §. 178, X; so ist zuvörderst

$D = 3$, $Q_0 = -1$, $K = \frac{\sqrt{3} + 0}{-1}$

m	P_m	Q_m	$(-1)^m Q_m$	a_m	M_m	N_m
−2					0	1
−1		−3	3		1	0
0	0	−1	−1	−2	−2	1
1	2	1	−1	3	−5	3
2	1	2	2	1		
3	1	1	−1	2		
4	1	2	2	1		

Ein Quadrat kommt unter den Grössen $(-1)^m Q_m$ nicht vor. Nehmen wir für q die kleinste darunter vorkommende positive Zahl 2; so haben wir $m=2$, $P_m=1$, $Q_m=2$, $(-1)^m Q_m = q = 2$, $M_{m-1} = -5$, $N_{m-1}=3$, $M_{m-2}=-2$, $N_{m-2}=1$ und die erste transformirte Gleichung ist

$$x'^2 - 3y'^2 = 2(z^2 - 7t^2)$$

oder wenn mit 2 multiplizirt wird,

$$2(x'^2 - 3y'^2) = (2z)^2 - 7(2t)^2 = z'^2 - 7t'^2$$

Kehrt man dieselbe um; so ist für

$$z'^2 - 7t'^2 = 2(x'^2 - 3y'^2)$$

$K' = \frac{\sqrt{7} + P_0}{2}$ zu entwickeln. Hierfür kann $P_0 = \pm 1$ genommen werden. Nimmt man $P_0 = 1$; so kommt $K = \frac{\sqrt{7} + 1}{2}$

m'	$P'_{m'}$	$Q'_{m'}$	$(-1)^{m'} Q_{m'}$	$a'_{m'}$	$M'_{m'}$	$N'_{m'}$
−2					0	1
−1		3	−3		1	0
0	1	2	2	1	1	1
1	1	3	−3	1	2	1
2	2	1	1			

Jetzt kann man bei $m' = 2$ schliessen, indem man hat $P'_{m'} = 2$, $Q'_{m'} = 1$, $(-1)^{m'} Q'_{m'} = q' = 1$, $M'_{m'-1} = 2$, $N'_{m'-1} = 1$, $M'_{m'-2} = 1$, $N'_{m'-2} = 1$. Die Schlussgleichung ist hiernach

$$z''^2 - 7t''^2 = x'^2 - 3y'^2 \quad \text{oder}$$

$$z''^2 - x'^2 = 7t''^2 - 3y'^2$$

woraus nach §. 179

$$z'' = \frac{u}{2p}(p^2 + 7v^2 - 3w^2), \quad x' = \frac{u}{2p}(p^2 - 7v^2 + 3w^2)$$
$$t'' = uv, \quad y' = uw$$

folgt.

Die rückgängigen Substitutionen liefern zunächst

$$\mathfrak{M}'_{n'} = \frac{z'' + P'_{m'}t''}{Q'_{m'}} = z'' + 2t'', \quad \mathfrak{N}'_{n'} = t''$$
$$M'_{m'+n'} = M'_{m'-1}\mathfrak{M}'_{n'} + M'_{m'-2}\mathfrak{N}'_{n'} = 2z'' + 5t''$$
$$N'_{m'+n'} = N'_{m'-1}\mathfrak{M}'_{n'} + N'_{m'-2}\mathfrak{N}'_{n'} = z'' + 3t''$$
$$z' = Q_0'M'_{m'+n'} - P_0'N'_{m'+n'} = 3z'' + 7t''$$
$$t' = N'_{m'+n'} = z'' + 3t''$$

Jetzt ist

$$z = \frac{z'}{2} = \frac{3z'' + 7t''}{2}, \quad t = \frac{t'}{2} = \frac{z'' + 3t''}{2}$$

und man hat nun weiter

$$\mathfrak{M}_n = \frac{x' + P_m y'}{Q_m} = \frac{x' + y'}{2}, \quad \mathfrak{N}_n = y'$$
$$M_{m+n} = M_{m-1}\mathfrak{M}_n + M_{m-2}\mathfrak{N}_n = -\frac{5x' + 9y'}{2}$$
$$N_{m+n} = N_{m-1}\mathfrak{M}_n + N_{m-2}\mathfrak{N}_n = \frac{3x' + 5y'}{2}$$
$$x = Q_0 M_{m+n} - P_0 N_{m+n} = \frac{5x' + 9y'}{2}$$
$$y = N_{m+n} = \frac{3x' + 5y'}{2}$$

Führt man in die letzteren Ausdrücke für x, y, z, t die aus der Schlussgleichung gefundenen Werthe für x', y', z'', t'' ein; so ergibt sich die Auflösung

$$x = \frac{u}{4p}[5(p^2 - 7v^2 + 3w^2) + 18pw]$$
$$y = \frac{u}{4p}[3(p^2 - 7v^2 + 3w^2) + 10pw]$$
$$z = \frac{u}{4p}[3(p^2 + 7v^2 - 3w^2) + 14pv]$$
$$t = \frac{u}{4p}[p^2 + 7v^2 - 3w^2 + 6pv]$$

Setzt man z. B. $v = 0$, $w = 0$, $p = 1$, $u = 4$; so erhält man $x = 5$, $y = 3$, $z = 3$, $t = 1$.

§. 183. **Behandlung der allgemeinsten Form der homogenen Gleichung mit vier Unbekannten.**

I. Eine solche Gleichung sei in der Gestalt

(1) $ax^2+by^2+cz^2+dt^2+2exy+2fxz+2gxt+2hyz+2iyt+2kzt=0$

gegeben, worin die Koeffizienten der Produkte von je zwei Unbekannten paare Zahlen seien. Es kommt uns zunächst darauf an, diese Gleichung in die Form der in §. 178 behandelten Gleichung zu bringen, welche nur Quadrate von vier Unbekannten enthält. Das hierauf abzielende Verfahren, welches auch auf homogene Gleichungen mit mehr als vier Unbekannten anwendbar ist, besteht in Folgendem.

II. Man multiplizirt zuvörderst mit dem Koeffizienten eines Quadrates der in Gl. (1) vorkommenden Unbekannten, also etwa mit a. Hierdurch erhält man, wenn man zur Abkürzung

(2) $$X=ax+ey+fz+gt$$

(3) $$\begin{cases} A=ab-e^2, & B=ac-f^2, & C=ad-g^2, \\ D=ah-ef, & E=ai-eg, & F=ak-fg \end{cases}$$

setzt,

(4) $$X^2+Ay^2+Bz^2+Ct^2+2Dyz+2Eyt+2Fzt=0$$

III. Die Glieder dieser Gleichung, mit Ausschluss des ersten, haben nun eine der gegebenen Gleichung ähnliche Form; dieselben enthalten jedoch nur drei Unbekannte. Wendet man auf diese Glieder das obige Multiplikationsverfahren an, indem man etwa mit A multiplizirt; so kommt, wenn man zur Abkürzung

(5) $$Y=Ay+Dz+Et$$

(6) $$G=AB-D^2,\quad H=AC-E^2,\quad I=AF-DE$$

setzt,

(7) $$AX^2+Y^2+Gz^2+Ht^2+2Izt=0$$

IV. Die Glieder dieser Gleichung, mit Ausschluss der ersten beiden, besitzen wiederum die ursprüngliche Form, jedoch nur mit zwei Unbekannten. Multiplizirt man also in der früheren Weise mit G, und setzt zur Abkürzung

(8) $$Z=Gz+It$$

(9) $$K=GH-I^2$$

so kommt

(10) $$AGX^2+GY^2+Z^2+Kt^2=0$$

V. Diese reduzirte Gleichung ist nun in Beziehung zu den vier Unbekannten X, Y, Z, t von der gewünschten Form, und kann nach §. 178 behandelt werden. Nachdem man die allgemeinen Ausdrücke für diese Unbekannten gefunden hat,

ergeben sich die für x, y, z, t vermöge der Beziehungen (8), (5), (2), indem man hiernach hat

$$(11) \qquad \begin{cases} t = t \\ z = \frac{1}{G}(Z - It) \\ y = \frac{1}{A}(Y - Dz - Et) \\ x = \frac{1}{a}(X - ey - fz - gt) \end{cases}$$

Da eine willkürliche Grösse u als Faktor von x, y, z, t erscheinen wird; so leuchtet ein, dass man stets ganze Werthe für diese Unbekannten darstellen kann, wenn sonst nur die Gl. (10) lösbar ist.

VI. Es muss darauf aufmerksam gemacht werden, dass wenn die Grösse A den negativen Werth eines Quadrates ergeben sollte, man die Transformation schon bei der Gl. (7) abbrechen kann, weil sich dann diese Gleichung sofort für X, Y, z, t nach §. 177 auflösen lässt, indem man die X und Y enthaltenden Glieder links stehen lässt, die z und t enthaltenden aber auf die rechte Seite stellt und $z = uv$, $t = uw$ setzt.

Ein ähnliches Verfahren kann überhaupt dann angewandt werden, wenn von den drei Grössen A, B, C irgend Eine den negativen Werth eines Quadrates annimmt, indem man alsdann mit dieser Grösse die Gl. (4) multiplizirt.

VII. Ferner leuchtet ein, dass die Transformation bei der Gl. (4) ihr Ende erreicht, wenn gleichzeitig $D = 0$, $E = 0$, $F = 0$ wird, oder bei der Gl. (7), wenn sich $I = 0$ ergibt.

§. 184. *Spezielle Fälle der vorstehend behandelten Gleichung.*

I. Fehlte in der allgemeinen Gleichung des vorhergehenden Paragraphen das Quadrat von x, wäre also $a = 0$; so wäre offenbar die Multiplikation mit a unzulässig. Man müsste dann mit dem Koeffizienten eines vorhandenen Quadrates, also entweder mit b, c oder d multipliziren.

Fehlten aber die Quadrate aller Unbekannten, wäre also $a = 0$, $b = 0$, $c = 0$, $d = 0$; so brauchen die Koeffizienten der übrigen Glieder nicht zu paaren Zahlen gemacht zu werden. Die gegebene Gleichung sei also einfach

$$(1) \qquad exy + fxz + gxt + hyz + iyt + kzt = 0$$

Multiplizirt man dieselbe mit Einem der Koeffizienten, welcher nicht $= 0$ ist, z. B. mit e; so erhält man

$$(2) \quad (ex + hz + it)(ey + fz + gt) = fhz^2 + git^2 + (fi + gh - ek)zt$$

Setzt man jetzt

(3) $z = uv, \qquad t = uw$

(4) $X = ex + hz + it, \qquad Y = ey + fz + gt$

so hat man

(5) $XY = u^2[fhv^2 + giw^2 + (fi + gh - ek)vw]$

Bezeichnet nun p irgend einen Faktor der in Klammern geschlossenen Grösse auf der rechten Seite, oder auch eine völlig willkürliche ganze Zahl; so kann man nehmen

(6) $Y = up, \qquad X = \frac{u}{p}[fhv^2 + giw^2 + (fi + gh - ek)vw]$

Vermöge der Beziehungen (3), (4) und (6) hat man alsdann die Auflösung

$$(7)\begin{cases} t = uw, \qquad z = uv \\ y = \frac{u}{e}(p - fv - gw) \\ x = \frac{u}{ep}[fhv^2 + giw^2 + (fi + gh - ek)vw - hpv - ipw] \end{cases}$$

Beispiel: $xy - 2xz + 3xt - yz - 5yt + 2zt = 0$

Die Auflösung (7) wird hier

$$t = uw, \qquad z = uv$$
$$y = u(p + 2v - 3w)$$
$$x = \frac{u}{p}(2v^2 - 15w^2 + 5vw + pv + 5pw)$$

Nimmt man einmal $p = 1$, $v = 1$, $w = 1$, $u = 1$; so kommt

$$t = 1, \qquad z = 1, \qquad y = 0, \qquad x = -2$$

Es wird noch darauf aufmerksam gemacht, dass in dem vorstehenden Falle I., wo von den Koeffizienten a, b, c, d Einer oder mehrere oder alle $= 0$ sind, von irgend einer Unbekannten nur die erste Potenz in der gegebenen Gleichung vorkommt; dass sich also diese Gleichung auch nach der einfachen Regel des §. 174 lösen lässt.

II. Wäre $A = 0$; so wäre eine Multiplikation der Gl. (4) im vorhergehenden Paragraphen mit A unzulässig. Man müsste dann mit B oder C multipliziren.

Wäre aber gleichzeitig $A = 0$, $B = 0$, $C = 0$; so reduzirt sich die Gl. (4) im vorhergehenden Paragraphen auf

(8) $X^2 = -2(Dyz + Eyt + Fzt)$

Hätte man jetzt auch $D = 0$, $E = 0$, $F = 0$; so läge, wenn man die Quadratwurzel auszieht, in der Form

(9) $X = ax + ey + fz + gt = 0$

eine diophantische Gleichung vom ersten Grade mit vier Unbekannten vor, welche nach dem zweiten Abschnitte aufgelös't werden kann.

Hätten von den drei Koeffizienten D, E, F nur zwei, z. B. D und E, den Werth null; so nähme die Gl. (8) die Form

(10) $$X^2 = -2Fzt$$

an, und man könnte setzen

(11) $$X = ax + ey + fz + gt = uvw$$

folglich

$$uv^2 . uw^2 = -2Fz . t$$

Hieraus ergibt sich

$$t = uw^2, \qquad -2Fz = uv^2, \quad \text{also} \quad z = -\frac{uv^2}{2F}$$

Durch diese beiden Formeln ist z und t bestimmt, und aus der Beziehung (11) kann noch x oder y gefunden werden. Hieraus erhellet, dass von den letzteren beiden Grössen x und y die Eine willkürlich bleibt. Setzt man also $y = ur$, worin auch r eine beliebige ganze Zahl darstellt; so hat man die Auflösung

(12) $$\begin{cases} t = uw^2, \qquad z = -\dfrac{uv^2}{2F}, \qquad y = ur \\ x = \dfrac{u}{2aF}[fv^2 - 2F(gw^2 - vw + er)] \end{cases}$$

Hätte von den drei Koeffizienten D, E, F nur Einer, z. B. D, den Werth null; so nähme die Gl. (8) die Form

(13) $$X^2 = -2(Ey + Fz)t$$

an, und man könnte setzen

(14) $$X = ax + ey + fz + gt = uvw$$

folglich

$$uv^2 . uw^2 = -2(Ey + Fz)t$$

Hieraus ergibt sich

$$-2(Ey + Fz) = uv^2, \qquad t = uw^2$$

Durch diese beiden Formeln ist t und von y und z die Eine bestimmt, während die andere willkürlich bleibt. Setzt man also $y = ur$, worin r eine beliebige ganze Zahl bezeichnet; so erhält man unter Berücksichtigung der Gl. (14) die Auflösung

(15) $$\begin{cases} t = uw^2, \qquad z = -\dfrac{u}{2F}(v^2 + 2Er), \qquad y = ur \\ x = \dfrac{u}{2aF}[fv^2 - 2gFw^2 + 2Fvw + 2(fE - eF)r] \end{cases}$$

Hätte endlich keiner der drei Koeffizienten D, E, F den Werth null; so multiplizire man die Gl. (8) mit Einem derselben, z. B. mit D. Dies gibt

$$(16) \qquad DX^2 - 2EFt^2 = -2(Dy + Ft)(Dz + Et)$$

Setzt man nun

$$(17) \qquad X = ax + ey + fz + gt = uv, \qquad t = uw$$

so hat man

$$u^2(Dv^2 - 2EFw^2) = -2(Dy + Fuw)(Dz + Euw)$$

Bezeichnet jetzt p irgend einen Faktor der Grösse $Dv^2 - 2EFw^2$, oder auch überhaupt nur eine willkürliche ganze Zahl; so kann man nehmen

$$(18) \qquad \begin{cases} Dy + Fuw = up \\ -2(Dz + Euw) = \dfrac{u(Dv^2 - 2EFw^2)}{p} \end{cases}$$

Aus den vier Beziehungen (17) und (18) ergibt sich die Auflösung

$$(19) \qquad \begin{cases} t = uw, \qquad z = -\dfrac{u}{2Dp}(Dv^2 - 2EFw^2 + 2Epw) \\ y = \dfrac{u}{D}(p - Fw) \\ x = \dfrac{u}{2aDp}[fDv^2 - 2fEFw^2 - 2ep^2 + 2Dpv + 2(eF + fE - gD)pw] \end{cases}$$

Das letztere Multiplikationsverfahren mit Einem der Koeffizienten $D, E \ldots$ ist auch allgemein dann einzuschlagen, wenn die rechte Seite der Gl. (8) mehr als drei Unbekannte und mehr als zwei Glieder enthält.

Schliesslich bemerken wir, dass in dem vorstehenden Falle II, wo von den drei Koeffizienten A, B, C Einer oder mehrere $= 0$ sind, in der Gl. (4) des vorhergehenden Paragraphen von irgend Einer der Unbekannten y, z, t nur die erste Potenz vorkommt, dass sich also diese Gleichung auch nach der einfachen Vorschrift des §. 174 für X, y, z, t lösen lässt, woraus man mit Hülfe der Gl. (2) im vorhergehenden Paragraphen auch leicht den Werth von x findet.

III. **Wäre $G = 0$; so wäre die Multiplikation der Gl. (7) im vorhergehenden Paragraphen mit G unzulässig. Man müsste dann mit H multipliziren.**

Wäre aber gleichzeitig $G = 0$ und $H = 0$, ohne dass zugleich $I = 0$ wäre; so reduzirte sich jene Gleichung auf

$$(20) \qquad AX^2 + Y^2 = -2Izt$$

Setzt man jetzt

(21) $\begin{cases} X = ax + ey + fz + gt = uv \\ Y = Ay + Dz + Et = uw \end{cases}$

so hat man

$$u^2(Av^2 + w^2) = -2Izt$$

und wenn p irgend einen Faktor von $Av^2 + w^2$, oder auch eine völlig willkürliche Zahl bezeichnet,

$$t = up, \qquad -2Iz = \frac{u(Av^2 + w^2)}{p}$$

Hieraus und aus den beiden Gleichungen (21) folgt die Auflösung

(22) $\begin{cases} t = up, \qquad z = -\dfrac{u(Av^2 + w^2)}{2Ip} \\ y = \dfrac{u}{2AIp}\,[D(Av^2 + w^2) + 2I(pw - Ep^2)] \\ x = \dfrac{u}{2aAIp}\,[(fA - eD)(Av^2 + w^2) + 2I(eE - gA)p^2 + 2AIpv - 2eIpw] \end{cases}$

Wäre ausser $G = 0$ und $H = 0$ auch $I = 0$; so reduzirte sich die obige Gl. (20) auf

(23) $$AX^2 + Y^2 = 0$$

Damit dieselbe lösbar sei, muss nothwendig A der negative Werth eines Quadrates sein; man muss also $A = -\alpha^2$ haben. Alsdann ist aber $\alpha^2X^2 = Y^2$, also $\alpha X = \mp Y$ oder $\alpha X \pm Y = 0$, d. i. wegen der Werthe von X und Y

(24) $$\alpha ax + (\alpha e \pm A)y + (\alpha f \pm D)z + (\alpha g \pm E)t = 0$$

worin gleichzeitig die oberen oder die unteren Zeichen zu nehmen sind. Man erkennt, dass hierdurch die gegebene Gleichung auf zwei diophantische Gleichungen vom ersten Grade mit vier Unbekannten zurückgeführt ist, welche nach dem zweiten Abschnitte aufgelös't werden können.

Auch für den vorstehenden Fall III., wo von den Koeffizienten G, H dieser oder jener $= 0$ ist, also in der Gl. (7) des vorhergehenden Paragraphen von den beiden Unbekannten z, t irgend Eine nur auf erster Potenz vorkommt, ist es von Wichtigkeit, dass auf diese Gleichung (insofern nicht auch $I = 0$ ist) das einfache Auflösungsverfahren des §. 174 angewandt werden kann, wodurch man die Werthe für X, Y, z, t findet, welche vermöge der Beziehungen (2) und (5) des vorigen Paragraphen auch zu den Werthen von x, y führen.

IV. Wäre $K = 0$; so enthielte die Schlussgleichung (10) im vorhergehenden Paragraphen nur die drei Unbekannten X, Y, Z und wäre mithin nach dem siebenten Abschnitte für X, Y, Z aufzulösen. Es leuchtet ein, dass alsdann irgend Eine

der Unbekannten x, y, z, t, z. B. t, ganz willkürlich bleibt. Bezeichnet dann u den willkürlichen Faktor in den für X, Y, Z sich ergebenden Ausdrücken; so kann man $t = up$ setzen, worin auch p willkürlich bleibt.

V. Es ist beachtenswerth, dass alle im gegenwärtigen Paragraphen bezeichneten Fälle, mit Ausnahme der Spezialität $G = 0$, $K = 0$, $I = 0$ sub III. und des Falles IV., unbedingt lösbar sind. Nur die letzteren beiden Spezialitäten können zuweilen unmöglich sein, was man jedoch für die erste Spezialität sofort, und für die zweite nach dem siebenten Abschnitte leicht erkennt.

Homogene Gleichungen mit beliebig vielen Unbekannten in ganzen Zahlen.

§. 185. ***Behandlung derselben behuf Erzielung einer Auflösung.***

I. Besitzt die gegebene Gleichung mit beliebig vielen Unbekannten x, y, z... ausser den Quadraten der Unbekannten auch Produkte aus je zwei derselben; so kann man dieselbe nach §. 183 auf eine andere mit den Unbekannten X, Y, Z... zurückführen, von welcher nur die Quadrate vorkommen.

Die ersten und die letzten Unbekannten werden stets durch Beziehungen vom ersten Grade miteinander verbunden sein, wie Gl. (2), (5), (8)... in §. 183. Kann man also die reduzirte Gleichung für X, Y, Z... lösen, wobei jede Unbekannte denselben willkürlichen Faktor enthalten wird; so kann man auch leicht die Werthe für x, y, z... herstellen, welche denselben Faktor besitzen, sich also stets zu ganzen Zahlen machen lassen.

II. Käme in der gegebenen oder in irgend Einer der reduzirten Gleichungen, welche bei dem Verfahren des §. 183 nach und nach auftreten, irgend Eine Unbekannte nur auf erster Potenz vor; so könnte man die Lösung dieser Gleichung nach §. 174 mit Sicherheit bewirken, und darauf auch die Werthe für x, y, z... darstellen.

Ereignet sich jedoch dieser besondere Fall nicht; so hat man die reduzirte Gleichung, welche von der Form

$$(1) \qquad ax^2 + by^2 + cz^2 + dt^2 + es^2 + \ldots = 0$$

ist, in einer Weise zu behandeln, welche der in §. 178 beschriebenen ganz ähnlich ist.

III. Zuvörderst sieht man nach, ob irgend zwei Glieder der Gl. (1) die Differenz zweier Quadrate bilden, oder ob Dies durch Multiplikation mit einer konstanten Zahl erreicht werden

kann. Ist Dies der Fall; so kann die Gl. (1) sofort nach §. 177 gelös't werden. Denn wäre

(2) $$\alpha^2x^2 - \beta^2y^2 = cz^2 + dt^2 + es^2 + \ldots$$

so setze man

(3) $$z = ru, \qquad t = rv, \qquad s = rw \quad \text{etc.}$$

Hierdurch wird Gl. (2)

$$(\alpha x + \beta y)(\alpha x - \beta y) = r^2(cu^2 + dv^2 + ew^2 + \ldots)$$

Jetzt setze man

(4) $$\alpha x + \beta y = rp$$

(5) $$\alpha x - \beta y = \frac{r(cu^2 + dv^2 + ew^2 + \ldots)}{p}$$

worin p irgend einen Faktor der Grösse $cu^2 + dv^2 + ew^2 + \ldots$ oder auch eine völlig willkürliche Zahl bezeichnet.

Hieraus folgt

(6) $$x = \frac{r(p^2 + cu^2 + dv^2 + ew^2 + \ldots)}{2\alpha p}$$

(7) $$y = \frac{r(p^2 - cu^2 - dv^2 - ew^2 - \ldots)}{2\beta p},$$

Diese beiden und die drei Formeln (3) stellen die Auflösung der Gl. (2) dar.

IV. Hat nun nicht schon die gegebene Gl. (1) die Form (2); so sucht man dieselbe durch die in §. 178 beschriebenen Transformationen auf eine solche Form zu bringen. Zu dem Ende wählt man sich von den n Gliedern, aus welchen die linke Seite der Gl. (1) besteht, irgend 4 aus, und behandelt dieselben genau so, wie die vier Glieder der in §. 178 betrachteten Gleichung, indem man die übrigen $n-4$ Glieder der Gl. (1) fortwährend auf der rechten Seite stehen lässt. Diese $n-4$ Glieder werden dann ebenso, wie das in z^2 multiplizirte Glied in §. 178 bei allen Transformationen dieselben Unbekannten behalten und nur ihre Koeffizienten ändern.

Der erste Schritt der nach §. 178 vorzunehmenden Entwickelung besteht also darin, dass man die gegebene Gleichung in der Form

(8) $$ax^2 - by^2 = cz^2 + dt^2 + es^2 + \ldots$$

schreibt, und hieraus durch Multiplikation mit ac^2 die Form

(9) $$(acx)^2 - abc^2y^2 = ac[(cz)^2 + cdt^2 + ces^2 + \ldots]$$

herstellt. Sollten a und c quadratische Faktoren oder ein gemeinschaftliches Maass enthalten; so kann man nach §. 178, I., anstatt mit ac^2, mit der kleineren Zahl $AC^2\mu$ multipliziren.

Die erste transformirte Gleichung nimmt, wenn hier, wie in §. 162, die Grösse $K = \frac{\sqrt{abc^2} + P_0}{ac}$ in einen Kettenbruch entwickelt wird, die Gestalt

(10) $$x'^2 - abc^2y'^2 = q[(cz)^2 + cdt^2 + ces^2 + \ldots]$$

an. Ist nun $(-1)^m Q_m = q$ ein Quadrat; so ist diese Gleichung die Schlussgleichung, welche wie die obige Gl. (2) aufgelös't werden kann. Findet sich jedoch unter den Grössen $(-1)^m Q_m$ kein Quadrat; so transponiren wir, wie in §. 178, immer die zweiten Glieder auf beiden Seiten. Dies gibt

(11) $$-cdqt^2 + x'^2 = q(cz)^2 + abc^2y'^2 + q[ces^2 + \ldots]$$

und nach Multiplikation mit $-cdq$

(12) $$(cdqt)^2 - cdqx'^2 = -cd\{(cqz)^2 + abc^2qy'^2 + q^2[ces^2 + \ldots]\}$$

Indem man jetzt $K' = \frac{\sqrt{cdq} + P_0'}{-cd}$ in einen Kettenbruch entwickelt, gelangt man zu der zweiten transformirten Gleichung

(13) $$x''^2 - cdqy''^2 = q'\{(cqz)^2 + abc^2qy'^2 + q^2[ces^2 + \ldots]\}$$

u. s. w.

V. Aus Vorstehendem erkennt man, dass die gegebene Gl. (1) jedenfalls dann lösbar ist, wenn die aus den vier Gliedern $ax^2 + by^2 + cz^2 + dt^2 = 0$ gebildete Gleichung mit vier Unbekannten lösbar ist.

Allgemein ist klar, dass wenn sich aus den n Gliedern der gegebenen Gleichung irgend welche m Glieder herausnehmen lassen und für sich eine lösbare Gleichung bilden, auch die gegebene lösbar ist und leicht gelös't werden kann.

Ausserdem erhellet, dass man in jeder transformirten Gleichung wie (10) statt des Gliedes $cdqt^2$ irgend Eines der darauf folgenden transponiren kann, was zuweilen die Lösung herbeiführt, wenn die Transposition des erst genannten Gliedes nicht zum Ziele führt.

Ferner kann auch hier die in §. 178, X. beschriebene Transformation ausgeführt werden, indem man die an der Verwandlung der Unbekannten nicht Theil nehmenden $n-4$ Glieder immer auf die rechte Seite transponirt.

§. 186. **Beispiel:**

$$x^2 + y^2 + z^2 + s^2 = 770t^2$$

Da nach §. 162 die durch Wegwerfung des Gliedes s^2 entstehende Gleichung lösbar ist; so ist es auch die gegenwärtige. Schreiben wir wie dort

$$x^2 - 770t^2 = -1(y^2 + z^2 + s^2)$$

so ergibt sich genau derselbe Entwickelungsgang wie in §. 180.

Durch $K = \frac{\sqrt{770} + 0}{-1}$ gelangt man zu der ersten transformirten Gleichung

$$x'^2 - 770y'^2 = 41(y^2 + z^2 + s^2)$$

oder durch Transposition zu

$$41z^2 - x'^2 = -41y^2 - 770y'^2 - 41s^2$$

und wenn man mit 41 multiplizirt, zu

$$(41z)^2 - 41x'^2 = -1[(41y)^2 + 41\,.\,770y'^2 + (41s)^2]$$

Die Entwickelung von $K' = \frac{\sqrt{41} + 0}{-1}$ liefert dann die zweite transformirte Gleichung

$$x''^2 - 41y''^2 = 1[(41y)^2 + 41\,.\,770y'^2 + (41s)^2]$$

welche auch die Schlussgleichung ist. Dieselbe führt, wenn sie in die Form

$$x''^2 - (41y)^2 = 41y''^2 + 41\,.\,770y'^2 + (41s)^2$$

gestellt wird, nach §. 185, III. zu der Auflösung

$$x'' = \frac{r}{2p}[p^2 + 41(u^2 + 770v^2 + 41w^2)]$$

$$y = \frac{r}{82p}[p^2 - 41(u^2 + 770v^2 + 41w^2)]$$

$$y'' = ru, \quad y' = rv, \quad s = rw$$

Die rückgängigen Substitutionen sind denen in §. 180 ganz gleich; man findet also auch hier

$$z = \frac{32x'' + 205y''}{41}$$

$$x = \frac{83(5x'' + 32y'') + 14\,.\,85y'}{41}$$

$$t = \frac{3(5x'' + 32y'') + 43y'}{41}$$

Substituirt man hierin für x'', y'', y' die aus der Schlussgleichung gefundenen Werthe; so ergibt sich folgende Auflösung

$$x = -\frac{r}{82p}[5.83(p^2 + 41u^2 + 41.770v^2 + 41^2w^2) + 64.83pu + 28.85pv]$$

$$y = \frac{r}{82p}[p^2 - 41u^2 - 41\,.\,770v^2 - 41^2w^2]$$

$$z = \frac{r}{41p}[16(p^2 + 41u^2 + 41\,.\,770v^2 + 41^2w^2) + 5\,.\,41pu]$$

$$s = rw$$

$$t = \frac{r}{82p}[15(p^2 + 41u^2 + 41\,.\,770v^2 + 41^2w^2) + 6\,.\,32pu + 86pv]$$

Nimmt man einmal $u=0$, $v=0$, $w=1$, $p=1$, $r=82$; so kommt $x=-698030$, $y=-1680$, $z=53824$, $s=82$, $t=24480$, worin x und y auch positiv genommen werden können.

Allgemeine Gleichungen mit drei oder mehr Unbekannten in rationalen Zahlen.

§. 187. ***Behandlung derselben behuf Erzielung der Auflösung.***

Die Auflösung der homogenen Gleichungen mit n Unbekannten in ganzen Zahlen liefert sofort auch die Auflösung der allgemeinen Gleichungen mit $n-1$ Unbekannten in rationalen Zahlen, wie aus §. 176 leicht zu entnehmen ist. Man braucht nur, wenn $X, Y, Z\ldots$ die Unbekannten der gegebenen Gleichung sind, dieselben auf einerlei Benennung t gebracht zu denken, dann dafür resp. $\frac{x}{t}, \frac{y}{t}, \frac{z}{t}\ldots$ zu substituiren und die gegebene Gleichung mit t^2 zu multipliziren. Hierdurch ergibt sich eine homogene Gleichung mit den Unbekannten $x, z, z\ldots t,$ für welche ganze Zahlen gefunden werden müssen.

Um z. B. die Gleichung

$$X^2+Y^2+Z^2=770$$

welche Gauss in den *Disquisitiones arithmeticae, art. 292* in ganzen Zahlen gelös't hat, in rationalen Zahlen zu lösen, erhält man durch die bezeichnete Substitution die homogene Gleichung

$$x^2+y^2+z^2=770t^2$$

Diese Gleichung haben wir in §. 180 in ganzen Zahlen gelös't. Die dort gefundenen Werthe liefern folgende Auflösung in rationalen Zahlen:

$$X=\frac{x}{t}=-\frac{5.83(p^2+41v^2+41.770w^2)+64.83pv+28.85pw}{15(p^2+41v^2+41.770w^2)+6.32pv+86pw}$$

$$Y=\frac{y}{t}=\frac{p^2-41v^2-41.770w^2}{15(p^2+41v^2+41.770w^2)+6.32pv+86pw}$$

$$Z=\frac{z}{t}=\frac{32(p^2+41v^2+41.770w^2)+10.41pv}{15(p^2+41v^2+41.770w^2)+6.32pv+86pw}$$

So ergibt sich z. B. für $v=0$, $w=0$, $p=1$, $u=82$

$$X=\frac{83}{3},\qquad Y=\frac{1}{15},\qquad Z=\frac{32}{15}$$

Man erkennt, dass die gegebene Gleichung eine unendliche Menge rationaler Auflösungen zulässt, während die Menge der Auflösungen in ganzen Zahlen offenbar eine endliche ist.

Neunter Abschnitt.

Komplexe Zahlen und die daraus gebildeten Kettenbrüche und unbestimmten Gleichungen vom ersten Grade.

---

§. 188. *Grundbegriffe über die komplexen Zahlen. — Vollkommene Primzahlen.*

I. Die bisher betrachtete reelle Zahlform a ist von der komplexen Zahlform $a+b\sqrt{-1}$ nur ein spezieller Fall, welcher sich ergibt, wenn der absolute Werth des imaginären Theiles $b\sqrt{-1}$, oder wenn $b=0$ wird. Wir wollen jetzt die früheren Untersuchungen dadurch erweitern, dass wir dieselben auf die komplexen Zahlen ausdehnen. Zu dem Ende schreiben wir der Abkürzung wegen für das imaginäre Zeichen $+\sqrt{-1}$ den Buchstaben i, betrachten also Zahlen von der allgemeinen Form $a+bi$, worin a und b sowol positiv, wie negativ sein können.

II. Nach dieser Bezeichnung ist i, i^2, i^3, i^4 resp. $=+\sqrt{-1}$, -1, $-\sqrt{-1}$, $+1$. Es handelt sich bei den gegenwärtigen Untersuchungen vorzugsweise, und wenn das Gegentheil nicht ausdrücklich befürwortet ist oder aus der Rechnung selbstverständlich hervorgeht, um ganze Zahlen, d. h. um solche, für welche sowol a, als auch b, ganz sind.

Da bei einer komplexen Zahl stets zwei Zahlgrössen in Betracht kommen; so sind darauf die für reelle Zahlen gültigen Merkmale von paar und unpaar ohne eine besondere Nebenbestimmung nicht mehr anwendbar. Wir werden im Folgenden die komplexe Zahl $a+bi$

vollständig paar nennen, wenn a und b paar sind,
vollständig unpaar » a und b unpaar sind,
unvollständig paar » a paar und b unpaar ist,
unvollständig unpaar » a unpaar und b paar ist.

Da für jede reelle Zahl die Grösse $b=0$, also paar ist; so folgt, dass jede paare reelle Zahl vollständig paar, jede unpaare reelle Zahl dagegen unvollständig unpaar ist.

Dass jede Zahl sowol durch die positiv und negativ reelle, als auch durch die positiv und negativ imaginäre Einheit, also durch $+1$, -1, $+\sqrt{-1}$, $-\sqrt{-1}$ oder durch i^4, i^2, i, i^3 theilbar sei, leuchtet ein.

Ferner erkennt man, dass jede vollständig paare, also jede Zahl von der Form $2m+2ni$, durch die Zahl 2, welche zugleich die einfachste vollständig paare Zahl darstellt, theilbar ist.

Auch ist leicht zu zeigen, dass jede vollständig unpaare, also jede Zahl von der Form $2m+1+(2n+1)i$, durch die ganze Zahl $1+i$, welche zugleich die einfachste vollständig unpaare Zahl darstellt, theilbar ist. Denn der Quotient

$$\frac{2m+1+(2n+1)i}{1+i}=\frac{[2m+1+(2n+1)i](1-i)}{(1+i)(1-i)}$$
$$=\frac{2(m+n+1)+2(n-m)i}{2}=m+n+1+(n-m)i$$

ist eine ganze Zahl.

Wir bemerken hier noch, dass auch die paare Zahl 2, also überhaupt jede vollständig paare Zahl, durch $1+i$ theilbar ist, indem man $\frac{2}{1+i}=\frac{2(1-i)}{(1+i)(1-i)}=\frac{2(1-i)}{2}=1-i$ hat.

Dagegen ist leicht zu zeigen, dass keine unvollständig paare oder unpaare Zahl durch $1+i$ theilbar sei.

Bezeichnen wir symbolisch eine vollständig paare Zahl mit 00, eine vollständig unpaare mit 11, eine unvollständig paare mit 01 und eine unvollständig unpaare mit 10; so ergeben die drei Grundoperationen der Addition, Subtraktion und Multiplikation folgende Resultate

$00 \pm 00 = 00$	$00 \times 00 = 00$
$00 \pm 01 = 01$	$00 \times 01 = 00$
$00 \pm 10 = 10$	$00 \times 10 = 00$
$00 \pm 11 = 11$	$00 \times 11 = 00$
$01 \pm 01 = 00$	$01 \times 01 = 10$
$01 \pm 10 = 11$	$01 \times 10 = 01$
$01 \pm 11 = 10$	$01 \times 11 = 11$
$10 \pm 10 = 00$	$10 \times 10 = 10$
$10 \pm 11 = 01$	$10 \times 11 = 11$
$11 \pm 11 = 00$	$11 \times 11 = 00$

III. Eine vollkommene Primzahl wollen wir nun diejenige nennen, welche sich durch keine andere ganze Zahl,

ausser durch irgend eine Potenz von i und durch ihren eigenen Werth oder durch ein Produkt aus ihrem eigenen Werthe und irgend einer Potenz von i, ohne Rest theilen lässt.

Aus dem Vorstehenden erhellet, dass weder eine vollständig paare Zahl, noch eine vollständig unpaare Zahl, mit Ausnahme der Zahl $1+i$, eine vollkommene Primzahl sein kann.

IV. Unter dem absoluten oder numerischen Werthe einer Zahl $a+bi$ verstehen wir jetzt den absoluten Werth der Grösse $\sqrt{a^2+b^2}$, welche im Allgemeinen **keine ganze Zahl** sein wird. Das Quadrat dieses absoluten Werthes, also die Grösse a^2+b^2, heisst nach Gauss die Norm der Zahl $a+bi$.

Die Norm aller vollständig paaren oder unpaaren, also aller durch $1+i$ theilbaren Zahlen, ist paar; dagegen ist die Norm aller unvollständig paaren oder unpaaren, also aller durch $1+i$ untheilbaren Zahlen, unpaar.

Wenn der absolute Werth einer Zahl $=\sqrt{2}$, also ihre Norm $a^2+b^2=2$ sein soll; so muss der absolute Werth von a und b gleich 1 und die Zahl selbst entweder $=1+i$ oder $=-1+i=(1+i)i$ oder $=-1-i=(1+i)i^2$ oder $=1-i=(1+i)i^3$, also immer ein Produkt aus $1+i$ und einer Potenz von i sein.

Wenn der absolute Werth einer Zahl $=1$, also auch ihre Norm $a^2+b^2=1$ sein soll; so muss von den beiden Grössen a und b die Eine absolut $=1$ und die andere $=0$, also jene Zahl selbst entweder $=\pm 1$ oder $=\pm i$, d. h. irgend eine Potenz von i sein.

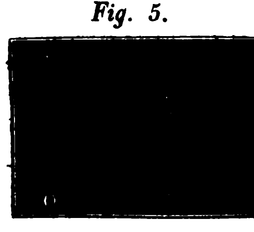
Soll der absolute Werth einer Zahl $=0$, also auch ihre Norm $a^2+b^2=0$ sein; so muss $a=0$ und $b=0$, mithin die fragliche Zahl selbst $=0$ sein.

Wird die gegebene Zahl in die Form

$$a+bi=\sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}}+\frac{b}{\sqrt{a^2+b^2}}i\right)$$

gebracht; so stellt bekanntlich bei der geometrischen Auffassung der Zahlen, wenn man in der seitstehenden Figur O zum Nullpunkte, OX zur positiv reellen, OY zur positiv imaginären Axe nimmt, ferner $ON=a$ und $NM=b$ macht, die linke Seite $a+bi$ der obigen Gleichung den rechtwinklig gebrochenen Linienzug $(ON)+(NM)$ dar. Die rechte Seite jener Gleichung stellt den nach Länge und Richtung aufgefassten Strahl (OM) dar, indem die Länge desselben $OM=\sqrt{a^2+b^2}$ und $\cos MON=\frac{a}{\sqrt{a^2+b^2}}$, ferner $\sin MON=\frac{b}{\sqrt{a^2+b^2}}$ ist.

Fig. 5.



V. Wir nennen eine Zahl $a+bi$ **absolut** oder **numerisch grösser, kleiner oder gleich** einer andern Zahl a_1+b_1i, wenn der absolute Werth $\sqrt{a^2+b^2}$ der ersteren grösser, kleiner oder gleich dem numerischen Werthe $\sqrt{a_1^2+b_1^2}$ der letzteren, oder wenn die Norm a^2+b^2 der ersteren grösser, kleiner oder gleich der Norm $a_1^2+b_1^2$ der letzteren ist.

Wenn jedoch bei einer solchen Vergleichung auf die reellen und imaginären Theile der beiden Zahlen gesehen werden soll; so könnte man schreiben

$$\begin{array}{llll} a+bi \geqq\geqq a_1+b_1i & \text{wenn } a \geqq a_1 & \text{und } b \geqq b_1 \\ a+bi \leqq\leqq a_1+b_1i & \quad » \quad a \leqq a_1 & \quad » \quad b \geqq b_1 \\ a+bi \geqq\leqq a_1+bi_1 & \quad » \quad a \geqq a_1 & \quad » \quad b \leqq b_1 \\ a+bi \leqq\geqq a_1+bi_1 & \quad » \quad a \leqq a_1 & \quad » \quad b \geqq b_1 \end{array}$$

wobei a, b, a_1, b_1 sowol positiv, wie negativ gedacht werden können (§. 42, IV.).

§. 189. *Beziehungen zwischen der Norm der Faktoren und des daraus entstehenden Produktes, sowie zwischen der Norm des Dividends und Divisors und des daraus entstehenden Quotienten.*

I. Setzt man das **Produkt** aus zwei Faktoren

(1) $$(a_1+b_1i)(a_2+b_2i)=A_2+B_2i$$

so hat man

(2) $$A_2=a_1a_2-b_1b_2, \qquad B_2=a_1b_2+a_2b_1$$

Hieraus folgt

(3) $$A_2^2+B_2^2=(a_1^2+b_1^2)(a_2^2+b_2^2)$$

Setzt man ferner das Produkt aus drei Faktoren

(4) $$(a_1+b_1i)(a_2+b_2i)(a_3+b_3i)=A_3+B_3i$$

so ist wegen Gl. (1)

$$(A_2+B_2i)(a_3+b_3i)=A_3+B_3i$$

also wegen der Beziehung (3)

(5) $$A_3^2+B_3^2=(A_2^2+B_2^2)(a_3^2+b_3^2)=(a_1^2+b_1^2)\ a_2^2+b_2^2)(a_3^2+b_3^2)$$

Allgemein erkennt man, dass die Norm eines Produktes aus beliebig vielen Faktoren gleich dem Produkte der Normen dieser Faktoren ist.

II. Wenn die n Faktoren eines solchen Produktes einander gleich sind und man setzt die **Potenz**

(6) $$(a+bi)^n=A+Bi$$

so ist nach Vorstehendem

(7) $$A^2+B^2=(a^2+b^2)^n$$

Hieraus ergibt sich umgekehrt, wenn $A+Bi$ die $n$te Wurzel von $a+bi$, also

(8) $$\sqrt[n]{a+bi}=A+Bi \text{ ist,}$$

(9) $$A^2+B^2=\sqrt[n]{a^2+b^2}$$

III. Was den Quotienten aus zwei komplexen Zahlen

(10) $$\frac{a+bi}{a_1+b_1i}=A+Bi$$

betrifft; so kann derselbe immer als der Quotient aus einem reellen Divisor und einem komplexen Dividend dargestellt werden. Zu dem Ende multiplizirt man den gegebenen Dividend und Divisor mit der Differenz der Theile des Divisors, also mit a_1-b_1i, wodurch der neue Divisor $=a^2+b^2$, also entschieden positiv und gleich der Norm des gegebenen Divisors wird. Diese Transformation wird bei den späteren Untersuchungen sehr häufig vorkommen und namentlich dann ohne besondere Erinnerung zur Ausführung gebracht werden, wenn es darauf ankommt, eine Division mit a_1+b_1i in $a+bi$ auszuführen. Man hat danach

(11) $$\frac{a+bi}{a_1+b_1i}=\frac{(a+bi)(a_1-b_1i)}{(a_1+b_1i)(a_1-b_1i)}=\frac{aa_1+bb_1}{a_1^2+b_1^2}+\frac{ba_1-ab_1}{a_1^2+b_1^2}i$$

also

(12) $$A=\frac{aa_1+bb_1}{a_1^2+b_1^2}, \qquad B=\frac{ba_1-ab_1}{a_1^2+b_1^2}$$

Soll der gegebene Dividend durch den Divisor theilbar, also der Quotient eine ganze Zahl sein; so muss A und B einen ganzen Werth haben, es muss also sowol aa_1+bb_1, als auch ba_1-ab_1 durch $a_1^2+b_1^2$ theilbar sein.

Aus den Werthen (12) für A und B folgt ferner

(13) $$A^2+B^2=\frac{a^2+b^2}{a_1^2+b_1^2}$$

Da nun A und B, folglich auch A^2+B^2 eine ganze Zahl ist; so leuchtet ein, dass a^2+b^2 durch $a_1^2+b_1^2$ theilbar sein muss. Diese Bedingung erfordert, dass

(14) $$a_1^2+b_1^2\leqq a^2+b^2$$

oder dass die Norm des Divisors kleiner oder gleich der des Dividends sei.

Wenn der Divisor nicht gerade eine Potenz von i ist, also nicht gerade den numerischen Werth 1 besitzt, wird entschieden

(15) $$A^2+B^2<a^2+b^2$$

oder es wird die Norm des Quotienten kleiner als die des Dividends sein.

§. 190. Sub- und Superquotienten. — Reste. — Absolut kleinste Reste.

I. Nach Vorstehendem hat man

$$(1)\qquad \frac{a+bi}{a_1+b_1i}=\frac{aa_1+bb_1}{a_1^2+b_1^2}+\frac{ba_1-ab_1}{a_1^2+b_1^2}i$$

Es sei gleichgültig, ob der Bruch auf der linken Seite einen ganzen Werth hat oder nicht. Im Allgemeinen werden die beiden Grössen $\frac{aa_1+bb_1}{a_1^2+b_1^2}$ und $\frac{ba_1-ab_1}{a_1^2+b_1^2}$ Brüche sein. Von jedem derselben kann man nach den betreffenden Gesetzen des ersten Abschnittes Sub- und Superquotienten absondern und die entstehenden Reste betrachten. Bezeichnet man einen solchen Quotienten für den ersten Bruch mit p, für den zweiten mit q, ferner den entstehenden Rest für den ersten Bruch mit r und für den zweiten mit s; so hat man

$$(2)\qquad \frac{aa_1+bb_1}{a_1^2+b_1^2}=p+\frac{r}{a_1^2+b_1^2}$$

$$(3)\qquad \frac{ba_1-ab_1}{a_1^2+b_1^2}=q+\frac{s}{a_1^2+b_1^2}$$

Hiernach ist der gegebene Bruch mit komplexem Zähler und Nenner

$$(4)\qquad \frac{a+bi}{a_1+b_1i}=p+qi+\frac{r+si}{a_1^2+b_1^2}$$

Multiplizirt man diese Gleichung mit dem Divisor a_1+b_1i; so erscheint der Dividend in der Form

$$(5)\qquad a+bi=(p+qi)(a_1+b_1i)+\frac{(r+si)(a_1+b_1i)}{a_1^2+b_1^2}$$

Da der Dividend $a+bi$ nach der Voraussetzung stets eine ganze Zahl ist; so muss auch nothwendig das letzte Glied auf der rechten Seite, welches sich in

$$(6)\qquad \frac{(r+si)(a_1+b_1i)}{a_1^2+b_1^2}=\frac{a_1r-b_1s}{a_1^2+b_1^2}+\frac{b_1r+a_1s}{a_1^2+b_1^2}i$$

auflös't, und welches sich auch, wenn man Zähler und Nenner mit a_1-b_1i multiplizirt, in der Form

$$(7)\qquad \frac{(r+si)(a_1+b_1i)}{a_1^2+b_1^2}=\frac{r+si}{a_1-b_1i}$$

schreiben lässt, eine ganze Zahl sein. Setzt man demnach dieses Glied, welches den Rest der Division mit a_1+b_1i in $a+bi$ darstellt, $=R+Si$, also nach Gl. (6)

$$(8)\qquad R=\frac{a_1r-b_1s}{a_1^2+b_1^2},\qquad S=\frac{b_1r+a_1s}{a_1^2+b_1^2}$$

so hat man statt (5)

(9) $$a + bi = (p + qi)(a_1 + b_1 i) + R + Si$$

Aus der Beziehung $R + Si = \frac{r + si}{a_1 - b_1 i}$ folgt auch nach dem vorhergehenden Paragraphen

(10) $$R^2 + S^2 = \frac{r^2 + s^2}{a_1^2 + b_1^2}$$

II. Um aus den gegebenen Zahlen $a + bi$ und $a_1 + b_1 i$ den in dieser Formel auftretenden Quotienten $p + qi$ und Rest $R + Si$ zu bestimmen, kann man folgendes Rechnungsverfahren beobachten.

Ist $p + qi$ ein willkürlicher Quotient; so ist der Rest einfach nach der Formel

(11) $$R + Si = a + bi - (p + qi)(a_1 + b_1 i)$$

zu berechnen.

Sind jedoch die Theile des Quotienten aus den Werthen (2) und (3) etwa als grösste Sub- oder kleinste Superquotienten zu bestimmen; so müssen zuerst die linken Seiten der Gleichungen (2), (3) dargestellt werden. In diesem Falle multiplizire man also erst den Zähler $a + bi$ mit $a_1 - b_1 i$, und nachdem auch $a_1^2 + b_1^2$ berechnet ist, bestimme man nach den gegebenen Bedingungen die Grösse p aus dem reellen Theile und die Grösse q aus dem imaginären Theile des Bruches $\frac{(a + bi)(a_1 - b_1 i)}{a_1^2 + b_1^2}$. Nachdem Dies geschehen, berechne man den Rest $R + Si$ nach der Formel (11), indem man $p + qi$ mit $a_1 + b_1 i$ multiplizirt und das Produkt von $a + bi$ subtrahirt.

Hiernach wird folgendes Rechnungsschema verständlich sein, worin der Bruch $\frac{16 + 21i}{7 + 2i}$ mit der Bedingung gegeben ist, dass p und q die grössten Subquotienten seien. Das Ganze ist in die Form der gewöhnlichen Division reeller Zahlen gebracht, indem die Berechnung der Quotienten p und q als eine Nebenrechnung seitwärts gestellt ist. Diese Nebenrechnung ist ebenfalls eine Division des mit $7 - 2i$ multiplizirten Nenners in den mit $7 - 2i$ multiplizirten Zähler.

$$7 + 2i \left| \begin{array}{l} 16 + 21i \\ \underline{10 + 18i} \\ 6 + 3i \end{array} \right| 2 + 2i \quad \Big\{ \times (7 - 2i) \Big\} \quad 53 \left| \begin{array}{l} 154 + 115i \\ \underline{106 + 106i} \\ 48 + 9i \end{array} \right| 2 + 2i$$

Hiernach ist $p + qi = 2 + 2i$, $R + Si = 6 + 3i$ und

$$16 + 21i = (2 + 2i)(7 + 2i) + 6 + 3i$$

und es ist auch

$$\frac{16+21i}{7+2i}=2+2i+\frac{48+9i}{53}$$

III. Wenn für p und q die grössten Subquotienten der Brüche (2) und (3) genommen werden; so ist klar, dass sowol r, als auch s entschieden positiv und $< a_1^2+b_1^2$, dass also auch

(12) $$r^2+s^2 < 2(a_1^2+b_1^2)^2$$

wird.

Was die Werthe von R und S anlangt; so folgt aus den Beziehungen (8) keineswegs, dass dieselben ebenfalls positiv werden müssten. Nach (10) hat man aber, wenn man beachtet, dass nach der vorstehenden Ungleicheit $\frac{r^2+s^2}{a_1^2+b_1^2} < 2(a_1^2+b_1^2)$ ist,

(13) $$R^2+S^2 < 2(a_1^2+b_1^2)$$

Es ist also nicht unbedingt gewiss, dass in dem gegenwärtigen Falle, wo p und q die grössten Subquotienten sind, die Norm R^2+S^2 des Restes kleiner sei, als die Norm $a_1^2+b_1^2$ des Divisors: vielmehr ist mit Gewissheit nur die Norm des Restes, also $R^2+S^2 < 2(a_1^2+b_1^2)$ oder der absolute Werth des Restes $\sqrt{R^2+S^2} < \sqrt{2(a_1^2+b_1^2)}$.

Ebendasselbe lässt sich sagen, wenn man für p und q die kleinsten Superquotienten der Brüche (2) und (3) annimmt, wodurch sowol r, als auch s negativ und absolut ebenfalls $< a_1^2+b_1^2$ wird.

IV. Wenn man für p und q, und zwar für jeden allein, ebensowol grösste Sub-, wie kleinste Superquotienten zulässt, und p und q unter der Bedingung bestimmt, dass die absoluten Werthe der Reste r und s in Gl. (2) und (3) so klein als möglich werden; so kann zwar sowol r, als s positiv und negativ werden: es muss jedoch der absolute Werth eines jeden $\leqq$ der Hälfte des Nenners, also $\leqq \frac{1}{2}(a_1^2+b_1^2)$, folglich

(13) $$r^2+s^2 \leqq \frac{1}{2}(a_1^2+b_1^2)$$

werden.

Was jetzt die Werthe von R und S betrifft; so hat man nach (10), da nun nach der vorstehenden Ungleichheit $\frac{r^2+s^2}{a_1^2+b_1^2} \leqq \frac{1}{2}(a_1^2+b_1^2)$ ist,

(14) $$R^2+S^2 \leqq \frac{1}{2}(a_1^2+b_1^2)$$

Entschieden ist also jetzt $R^2 + S^2 < a_1^2 + b_1^2$ und demnach die Norm des Restes kleiner als die des Divisors, oder der Rest absolut kleiner als der Divisor.

Diese Bestimmung der Quotienten p und q nach dem Prinzipe der absolut kleinsten Reste spielt die Hauptrolle in allen späteren Untersuchungen.

§. 191. ***Aufsuchung des grössten gemeinschaftlichen Maasses zweier Zahlen.***

Unter dem grössten gemeinschaftlichen Maasse zweier komplexen Zahlen $a + bi$ und $a_1 + b_1 i$ verstehen wir diejenige sowol in der ersten, wie in der zweiten aufgehende Zahl $p + qi$, deren Norm $p^2 + q^2$ am möglich grössten ist, oder auch diejenige, welche alle gemeinschaftlichen Faktoren der ersten und zweiten Zahl in sich vereinigt.

Um dieses grösste gemeinschaftliche Maass zu finden, bemerken wir zuvörderst, dass wenn die Normen $a^2 + b^2$ und $a_1^2 + b_1^2$ der gegebenen Zahlen nicht gleich sind, die Eine kleiner sein wird, als die andere. Es sei also $a_1^2 + b_1^2 \leqq a^2 + b^2$.

Hiernach wäre es möglich, dass die zweite Zahl $a_1 + b_1 i$ selbst das gesuchte grösste Maass sei. Dies prüft man, indem man mit $a_1 + b_1 i$ in $a + bi$ dividirt (wobei die im vorhergehenden Paragraphen sub I. bezeichnete Transformation ausgeführt wird.)

Geht diese Division nicht auf; so sondere man durch dieselbe nach dem vorhergehenden Paragraphen sub IV. denjenigen Quotienten $p_1 + q_1 i$ ab, für welchen der Rest, den wir mit $a_2 + b_2 i$ bezeichnen wollen, den kleinstmöglichen absoluten Werth annimmt. Alsdann kann man den Dividend in der Form

$$(1) \qquad (a + bi) = (p_1 + q_1 i)(a_1 + b_1 i) + a_2 + b_2 i$$

darstellen, worin $a_2^2 + b_2^2 \leqq \frac{1}{2}(a_1^2 + b_1^2)$ ist.

Das grösste gemeinschaftliche Maass von $a + bi$ und $a_1 + b_1 i$ ist nun auch das grösste gemeinschaftliche Maass von $a_1 + b_1 i$ und $a_2 + b_2 i$. Man setzt also die Ermittelung genau in der früheren Weise fort, indem man die letzten beiden Zahlen ebenso behandelt, wie die ersten beiden, also zunächst prüft, ob $a_2 + b_2 i$ das grösste gemeinschaftliche Maass ist oder in $a_1 + b_1 i$ aufgeht.

Insofern sich das Letztere nicht bestätigt, sondert man bei der Division mit $a_2 + b_2 i$ in $a_1 + b_1 i$ denjenigen Quotienten $p_2 + q_2 i$ ab, für welchen der Rest $a_3 + b_3 i$ den kleinstmöglichen absoluten Werth hat. Hierdurch wird

$$(2) \qquad a_1 + b_1 i = (p_2 + q_2 i)(a_2 + b_2 i) + a_3 + b_3 i$$

und man hat $a_3^2 + b_3^2 \leqq \frac{1}{2}(a_2^2 + b_2^2)$.

Jetzt ist das grösste gemeinschaftliche Maass von $a_2 + b_2 i$ und $a_3 + b_3 i$ zu suchen u. s. f.

Derjenige durch dieses Verfahren erreichte Divisor $a_n + b_n i$, welcher in dem vorhergehenden Dividende $a_{n-1} + b_{n-1} i$ aufgeht, ist das grösste gemeinschaftliche Maass von $a + bi$ und $a_1 + b_1 i$.

Wenn sich im Laufe dieser Rechnung kein in dem vorhergehenden Dividende aufgehender Divisor $a_n + b_n i$ ergibt, für welchen $a_n^2 + b_n^2 > 1$ ist; so muss, da die Zahlen $a^2 + b^2$, $a_1^2 + b_1^2$, $a_2^2 + b_2^2 \ldots$ eine stark abnehmende Reihe bilden, endlich ein Divisor auftreten, für welchen $a_n^2 + b_n^2 = 1$ ist. Dies ist nur möglich, wenn von den beiden Zahlen a_n und b_n die Eine $= \pm 1$ und die andere $= 0$ ist, wenn also $a_n + b_n i$ irgend eine Potenz von i, also entweder $= \pm 1$ oder $= \pm \sqrt{-1}$ ist. Mit diesem Divisor geht dann die letzte Division unbedingt auf, und es folgt, dass die gegebenen beiden Zahlen die positiv oder negativ reelle oder imaginäre Einheit zum grössten gemeinschaftlichen Maasse haben, oder vollkommen relativ prim sind.

Das vorstehende Divisionsverfahren nimmt in seinen Hauptzügen die Form des bei der Aufsuchung des grössten gemeinschaftlichen Maasses zwischen reellen Zahlen üblichen Verfahrens an, indem man die Nebenrechnungen nach dem vorhergehenden Paragraphen sub II. seitwärts schreibt.

Beispiel 1. Es soll das grösste gemeinschaftliche Maass zwischen $35+6i$ und $3+28i$ gesucht werden. Da $35^2+6^2=1261$, $3^2+28^2=793$ und $793<1261$ ist; so beginnt man mit der Division der zweiten Zahl in die erste. Dies liefert folgende Rechnung

$$\begin{array}{r|l|l l r|r|l}
3+28i & 35+6i & 0-i & \left\{\times(3-28i)\right\} & 793 & 273-962i & 0-i \\
 & & & & & 0-793i & \\
\cline{6-6}
28-3i & & & & & 273-169i & \\
\cline{1-1}
7+9i & 3+28i & 2+i & \left\{\times(7-9i)\right\} & 130 & 264+169i & 2+i \\
 & & & & & 260+130i & \\
\cline{6-6}
 & 5+25i & & & & 4+39i & \\
\cline{2-2}
-2+3i & 7+9i & 1-3i & \left\{\times(-2-3i)\right\} & 13 & 13-39i & 1-3i \\
 & & & & & 13-39i & \\
\cline{6-6}
 & 7+9i & & & & 0 & \\
\cline{2-2}
 & 0 & & & & &
\end{array}$$

Es ist also $-2+3i$ das grösste gemeinschaftliche Maass von $35+6i$ und $3+28i$.

Beispiel 2. Es soll das grösste gemeinschaftliche Maass zwischen $11+4i$ und $8-7i$ ermittelt werden. Da $11^2+4^2=137$, $8^2+7^2=113$ und $113<137$ ist; so dividiren wir zuerst mit der zweiten Zahl in die erste u. s. f. Dies gibt

$$\begin{array}{l}
8-7i \,|\, 11+4i \,|\, 0+i \quad \{\times(8+7i)\} \quad 113 \,|\, 60+109i \,|\, 0+i \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \underline{0+113i} \\
\underline{7+8i} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 60-\ \ 4i \\
\quad 4-4i \,|\, 8-7i \,|\, 2+0i \quad \{\times(4+4i)\} \quad 32 \,|\, 60+4i \,|\, 2+0i \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \underline{64+0i} \\
\qquad \underline{8-8i} \qquad\qquad\qquad\qquad\qquad\qquad\quad -4+4i \\
\qquad\qquad i \,|\, 4-4i \,|\, -4-4i \quad \{\times -i\} \quad 1 \,|\, -4-4i \,|\, -4-4i \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \underline{-4-4i} \\
\qquad\qquad \underline{4-4i} \qquad\qquad\qquad\qquad\qquad\qquad 0 \\
\qquad\qquad\quad 0
\end{array}$$

Da der letzte Divisor $=i$ ist; so folgt, dass $11+4i$ und $8-7i$ vollkommen relativ prim sind.

§. 192. ***Jede Zahl ist nur durch ihre vollkommenen Primfaktoren und durch Produkte daraus theilbar.***

I. **Wenn $p+qi$ eine vollkommene Primzahl und weder in $a+bi$, noch in a_1+b_1i enthalten ist; so ist sie auch nicht in dem Produkte $(a+bi)(a_1+b_1i)$ enthalten.**

Denn für den Fall, wo weder a^2+b^2, noch $a_1^2+b_1^2 < p^2+q^2$ ist, kann man nach §. 190, IV. setzen

(1) $$a_1+b_1i=(m+ni)(p+qi)+a_2+b_2i$$

worin $a_2^2+b_2^2 \leqq \frac{1}{2}(p^2+q^2)$, jedoch nicht $=0$ ist, da sonst $a_2=0$, $b_2=0$ sein, also $p+qi$ in a_1+b_1i aufgehen müsste, was der Voraussetzung widerspricht. Hiernach ist

(2) $$(a+bi)(a_1+b_1i)=(m+ni)(a+bi)(p+qi)+(a+bi)(a_2+b_2i)$$

Wäre nun $(a+bi)(a_1+b_1i)$ durch $p+qi$ theilbar; so müsste, da das erste Glied auf der rechten Seite durch $p+qi$ theilbar ist, es auch das zweite Glied oder $(a+bi)(a_2+b_2i)$ sein. Da in diesem Gliede für den Einen Faktor a_2+b_2i die Grösse $a_2^2+b_2^2<p^2+q^2$ ist; so entspricht die jetzt folgende Fortsetzung des Beweises zugleich dem Falle, wo für Eine der beiden **gegebenen** Zahlen $a_2^2+b_2^2<p^2+q^2$ wäre.

Man kann nun setzen

(3) $$p+qi=(m_2+n_2i)(a_2+b_2i)+a_3+b_3i$$

worin $a_3^2+b_3^2 \leqq \frac{1}{2}(a_2^2+b_2^2)$, jedoch nicht $=0$ ist, da sonst

$a_3 = 0$, $b_3 = 0$, also $a_2 + b_2 i$ ein Faktor von $p + qi$ sein müsste, was unmöglich ist, da $p = qi$ eine vollkommene Primzahl sein soll. Hiernach hat man

(4) $$(a+bi)(p+qi) = (m_2+n_2 i)(a+bi)(a_2+b_2 i) + (a+bi)(a_3+b_3 i)$$

Wäre nun $(a+bi)(a_2+b_2 i)$ durch $p+qi$ theilbar; so müsste, da die linke Seite hierdurch theilbar ist, auch $(a+bi)(a_3+b_3 i)$ es sein. Nun kann man ferner setzen

(5) $$p + qi = (m_3 + n_3 i)(a_3 + b_3 i) + a_4 + b_4 i$$

worin $a_4^2 + b_4^2 \leqq \frac{1}{2}(a_3^2 + b_3^2)$, jedoch nicht $= 0$ ist, und den vorhergehenden Schluss wiederholen, wonach $(a + bi)(a_4 + b_4 i)$ durch $p + qi$ theilbar sein müsste u. s. f.

Da $p^2 + q^2$, $a_1^2 + b_1^2$, $a_2^2 + b_2^2$, $a_3^2 + b_3^2 \ldots$ eine rasch fallende Reihe von Zahlen bilden; so muss man endlich auf ein Glied $a_r + b_r i$ dieser Reihe kommen, wofür $a_r^2 + b_r^2 = 1$, also $a_r + b_r i = \pm 1$ oder $= \pm i$ ist. Es müsste also $(a+bi)(\pm 1)$ oder $(a + bi)(\pm i)$, folglich auch $a + bi$ durch $p + qi$ theilbar sein, was der Voraussetzung widerspricht. Demnach kann auch das Produkt aus den beiden gegebenen Zahlen $a + bi$ und $a_1 + b_1 i$ nicht durch die Primzahl $p + qi$ theilbar sein.

Aus dem vorstehenden Satze folgt leicht, dass **jede Zahl nur durch ihre vollkommenen Primfaktoren und die daraus gebildeten Produkte, wobei jeder Primfaktor soviel Mal berücksichtigt werden kann, als er in der gegebenen Zahl selbst vorkommt, theilbar ist.**

§. 193. *Beziehungen zwischen den Theilen der Faktoren und den Theilen des daraus gebildeten Produkts.*

I. Um alle Zahlen in ihre vollkommenen Primfaktoren zu zerlegen, braucht man nur solche Zahlen $a + bi$ zu zerlegen, für welche a und b positiv sind. Die Primfaktoren der Zahlen von den Formen $a - bi$, $-a + bi$, $-a - bi$ ergeben sich dann leicht aus denen der ersteren Form, indem man allgemein hat, gleichviel, welche Zeichen a und b besitzen,

(1) $$a - bi = (b + ai)i^3$$

(2) $$-a + bi = (b + ai)i$$

(3) $$-a - bi = (a + bi)i^2$$

II. Von den Zahlen der Form $a + bi$ braucht man aber ferner nur diejenigen zu betrachten, in welchen $b \leqq a$ ist. Denn die Faktoren der Zahlen, in welchen $b > a$ ist, ergeben sich aus denen, in welchen $b \leqq a$ ist, leicht durch folgendes Gesetz.

Wenn man hat

(4) $A_1 + B_1 i = a_1 + b_1 i$

(5) $A_2 + B_2 i = (a_1 + b_1 i)(a_2 + b_2 i)$

(6) $A_3 + B_3 i = (a_1 + b_1 i)(a_2 + b_2 i)(a_3 + b_3 i)$

$\vdots$

(7) $A_n + B_n i = (a_1 + b_1 i)(a_2 + b_2 i) \ldots (a_n + b_n i)$

so ist allgemein, gleichviel, welche Zeichen und relativen Werthe die Grössen a_1, $a_2 \ldots$ b_1, $b_2 \ldots$ besitzen,

(8) $B_1 + A_1 i = b_1 + a_1 i$

(9) $B_2 + A_2 i = (b_1 + a_1 i)(b_2 + a_2 i) i^3$

(10) $B_3 + A_3 i = (b_1 + a_1 i)(b_2 + a_2 i)(b_3 + a_3 i) i^6$

$\vdots$

(11) $B_n + A_n i = (b_1 + a_1 i)(b_2 + a_2 i) \ldots (b_n + a_n i) i^{3(n-1)}$

Um die allgemeine Gültigkeit dieses Gesetzes darzuthun, zeigen wir zunächst, dass dasselbe für den Zeiger $n+1$ gelten werde, sobald dasselbe für den Zeiger n dargethan ist.

Setzen wir zu diesem Ende, indem F und G die Zeichen für zwei Funktionen sind,

(12) $(a_1+b_1 i)(a_2+b_2 i) \ldots (a_n+b_n i) = F_n(a,b) + G_n(a,b) . i = A_n + B_n i$

so ist unter Vertauschung von a und b

(13) $(b_1 + a_1 i)(b_2 + a_2 i) \ldots (b_n + a_n i) = F_n(b,a) + G_n(b,a) . i$

Nach der Voraussetzung soll aber sein

(14) $(b_1 + a_1 i)(b_2 + a_2 i) \ldots (b_n + a_n i) i^{3(n-1)}$

$= F_n(b,a) . i^{3(n-1)} + G_n(b,a) . i^{3(n-1)+1} = B_n + A_n i$

Jetzt ist zu unterscheiden, ob $3(n-1)$ paar oder unpaar ist.

Ist $3(n-1)$ paar oder n unpaar, also $i^{3(n-1)}$ reell; so hat man

$F_n(b,a) . i^{3(n-1)} = B_n, \qquad G_n(b,a) . i^{3(n-1)+1} = A_n i$

also

(15) $F_n(b,a) = B_n i^{3(n-1)}, \qquad G_n(b,a) = A_n i^{3(n-1)}$

Ist dagegen $3(n-1)$ unpaar oder n paar, also $i^{3(n-1)}$ imaginär; so hat man

$F_n(b,a) . i^{3(n-1)} = A_n i, \qquad G_n(b,a) . i^{3(n-1)+1} = B_n$

also

(16) $F_n(b,a) = A_n i^{3(n-1)-1}, \qquad G_n(b,a) = B_n i^{3(n-1)+1}$

Die Werthe vom Zeiger $n+1$ werden nun folgendermaassen erhalten. Es ist

(17) $(a_1+b_1 i) \ldots (a_{n+1}+b_{n+1}) = (A_n+B_n i)(a_{n+1}+b_{n+1} i)$

$= (a_{n+1} A_n + b_{n+1} B_n i^2)$

$+ (b_{n+1} A_n + a_{n+1} B_n) i$

$= [a_{n+1} F_n(a,b) + b_{n+1} G_n(a,b) . i^2]$

$+ [b_{n+1} F_n(a,b) + a_{n+1} G_n(a,b)] i$

$= A_{n+1} + B_{n+1} i$

Vertauscht man a und b; so kommt

(18) $(b_1+a_1i)\dots(b_{n+1}+a_{n+1}i) = [b_{n+1}F_n(b,a)+a_{n+1}G_n(b,a).i^2]$
$+[a_{n+1}F_n(b,a)+b_{n+1}G_n(b,a)]i$

Substituirt man hiervon für $F_n(b,a)$ und $G_n(b,a)$ die oben gefundenen Werthe; so ergibt sich, wenn n unpaar ist, nach (18) und (15)

$$(b_1+a_1i)\dots(b_{n+1}+a_{n+1}i) = [b_{n+1}B_n i^{3(n-1)}+a_{n+1}A_n i^{3(n-1)+2}] + [a_{n+1}B_n i^{3(n-1)}+b_{n+1}A_n i^{3(n-1)}]i$$

und wenn man beiderseits mit i^{3n} multiplizirt und die aus Gl. (17) zu ersehenden Werthe von A_{n+1} und B_{n+1} berücksichtigt,

(19) $(b_1+a_1i)\dots(b_{n+1}+a_{n+1}i)i^{3n} = [b_{n+1}A_n+a_{n+1}B_n]$
$+[a_{n+1}A_n+b_{n+1}B_ni^2]i = B_{n+1}+A_{n+1}i$

Wenn dagegen n paar ist; so hat man nach (18) und (16)

$$(b_1+a_1i)\dots(b_{n+1}+a_{n+1}i) = [b_{n+1}B_n i^{3(n-1)-1}+a_{n+1}B_n i^{3(n-1)+3}] + [a_{n+1}A_n i^{3(n-1)-1}+b_{n+1}B_n i^{3(n-1)+1}]i$$

und wenn man beiderseits mit i^{3n} multiplizirt und die aus Gl. (17) ersichtlichen Werthe von A_{n+1} und B_{n+1} berücksichtigt,

(20) $(b_1+a_1i)\dots(b_{n+1}+a_{n+1}i)i^{3n} = [b_{n+1}A_n+a_{n+1}B_n]$
$+[a_{n+1}A_n+b_{n+1}B_ni^2]i = B_{n+1}+A_{n+1}i$

Aus den Gleichungen (19) und (20) folgt, dass der angekündigte Satz für $n+1$ gilt, wenn er für n Gültigkeit hat. Da derselbe nun offenbar für $n=1$ seine Richtigkeit hat; so stellt er eine allgemeine Wahrheit dar.

III. Hätte man also durch Zerlegung gefunden, dass

(21) $A+Bi = i^m(a_1+b_1i)^{n_1}(a_2+b_2i)^{n_2}(a_3+b_3i)^{n_3}\dots$
$= (0+i)^m(a_1+b_1i)^{n_1}(a_2+b_2i)^{n_2}(a_3+b_3i)^{n_3}\dots$

wäre; so würde

(22) $B+Ai = i^{3(m+n_1+n_2+n_3+\dots-1)}(1+0i)^m(b_1+a_1i)^{n_1}(b_2+a_2i)^{n_2}\times(b_3+a_3i)^{n_3}\dots$
$= i^{3(m+n_1+n_2+n_3+\dots-1)}(b_1+a_1i)^{n_1}(b_2+a_2i)^{n_2}(b_3+a_3i)^{n_3}\dots$

sein, worin unter den Faktoren $a+bi$ offenbar auch reelle Grössen, für welche man $b=0$ hat, oder rein imaginäre, für welche man $a=0$ hat, vorkommen können.

So ist z. B.

$$925+400i = 5^2(3+2i)(2+i)^3$$

folglich ist

$$400+925i = i^{3(2+1+3-1)}(0+5i)^2(2+3i)(1+2i)^3$$
$$= i5^2(2+3i)(1+2i)$$

IV. Aus Vorstehendem ist auch leicht zu ersehen, dass aus der Beziehung

(23) $$A+Bi=(a_1+b_1i)\dots(a_n+b_ni)$$

die folgenden drei sich ergeben

(24) $$B+Ai=(b_1+a_1i)\dots(b_n+a_ni)i^{3(n-1)}$$

Ferner hat man

$$A-Bi=(B+Ai)i^3=(b_1+a_1i)\dots(b_n+a_ni)i^{3n}$$

wofür man auch schreiben kann

(25) $$A-Bi=(a_1-b_1i)\dots(a_n-b_ni)$$

Ferner ist

$$B-Ai=(A+Bi)i^3=(a_1+b_1i)\dots(a_n+b_ni)i^3$$

wofür man auch schreiben kann

(26) $$B-Ai=(b_1-a_1i)\dots(b_n-a_ni)i^{n-1}$$

Wenn die Faktoren in Gl. (23) einander gleich sind; so hat man

(27) $$A+Bi=(a+bi)^n$$

(28) $$B+Ai=(b+ai)^n i^{3(n-1)}$$

(29) $$A-Bi=(b+ai)^n i^{3n}$$
$$=(a-bi)^n$$

Wenn man also

(30) $$(a+bi)^n=A+Bi$$

hat; so ist

(31) $$(b+ai)^n=(B+Ai)i^{n-1}$$
$$=(A-Bi)i^n$$

V. Aus den obigen Sätzen ad I. ist klar, dass wenn $a+bi$ eine vollkommene Primzahl ist, auch $b+ai$, $a-bi$, und $b-ai$ vollkommene Primzahlen sind. Während sich jedoch $a-bi$ von $b+ai$ und $b-ai$ von $a+bi$ nur durch den Faktor i unterscheidet, ist $b+ai$ von $a+bi$ und $b-ai$ von $a-bi$ dergestalt verschieden, dass zwischen ihnen kein gemeinschaftliches Maass obwaltet.

Ferner erhellet, dass wennauch $a+bi$ und $b+ai$ zusammengesetzte Zahlen sind, doch niemals die Eine durch die andere theilbar sein kann, wennicht a oder $b=0$ oder wennnicht $a=b$ ist.

Man kann sogar behaupten, dass wenn $a+bi$ eine unvollständig paare oder unpaare Zahl, also weder durch 2, noch durch $1+i$, also auch nicht durch eine Zahl von der Form $p+pi$ theilbar ist, und wenn ausserdem a und b reelle relative Primzahlen sind, die beiden Zahlen $a+bi$ und $b+ai$ unter sich, ebensowie die beiden Zahlen $a-bi$ und $b-ai$ unter sich vollkommen relativ prim seien. Denn da

$$a+bi=(a_1+b_1i)(a_2+b_2i)\dots$$
$$b+ai=(b_1+a_1i)(b_2+a_2i)\dots$$

ist; so würde das Vorhandensein eines gemeinschaftlichen Maasses zwischen $a+bi$ und $b+ai$ die Gleichheit $a_1+b_1i = (b_1+a_1i)i^m$ bedingen, welche entweder $a_1=\pm b_1$, oder $a_1=0$, oder $b_1=0$ erfordert. Alle diese Fälle sind aber durch die Voraussetzung ausgeschlossen.

§. 194. *Charakteristische Merkmale der vollkommenen Primzahlen.*

I. Am Ende dieses Buches findet man eine Tafel der absoluten Werthe des reellen und des imaginären Theiles der vollkommenen Primzahlen $a+bi$ bis hinauf zur Norm $a^2+b^2=4001$. Jene absoluten Werthe von a und b können sowol positiv, wie negativ genommen, auch mit einander verwechselt werden. So ist z. B. für die Norm $8^2+3^2=73$ sowol $8+3i$, wie $8-3i$, wie $3+8i$, $3-8i$ u. s. w. eine vollkommene Primzahl.

Diese Tafel bekundet folgende wichtige Sätze über die vollkommenen Primzahlen.

Die Normen a^2+b^2 für die sukzessiv aufsteigenden **vollkommenen Primzahlen** sind sämmtlich **verschieden.** Sie enthalten die reelle Primzahl 2, ausserdem alle reellen Primzahlen von der Form $4n+1$ und endlich die Quadrate von den reellen Primzahlen der Form $4n+3$.

Die paare reelle Primzahl 2 stellt die Norm der vollkommenen Primzahl $1+1$ dar. Jede unpaare reelle Primzahl >1 von der Form $4n+1$ stellt die Norm einer vollkommenen Primzahl dar, in welcher weder a, noch b gleich null ist, welche also wirklich **komplex** ist. Jedes Quadrat von einer reellen Primzahl der Form $4n+3$ stellt die Norm einer vollkommenen Primzahl dar, in welcher $b=0$ ist, welche also selbst einen **reellen** Werth hat.

Hieraus erkennt man denn auch, dass die reelle Primzahl 2 und alle reellen Primzalen von der Form $4n+1$, welche >1 sind, dass also die Zahlen 2, 5, 13, 17, 29... **keine vollkommenen** Primzahlen sind, dass vielmehr unter den reellen Primzahlen nur die von der Form $4n+3$ **vollkommene** sind.

Der Beweis dieser Sätze lässt sich folgendermaassen führen.

II. Durch die Beziehung $i^3(1+i)^2=2$ sind die Sätze hinsichtlich der Zahl 2 erledigt.

III. Wenn $a+bi$, worin weder $a=0$, noch $b=0$, eine vollkommene Primzahl ist, also nur durch i^m oder durch

$i^m(a+bi)$ getheilt werden kann; so ist nach dem vorhergehenden Paragraphen, No. V., auch $b+ai$ eine vollkommene Primzahl. Mithin ist das Produkt aus beiden, nämlich $(a+bi)(b+ai) = (a^2+b^2)i$, also auch die reelle Zahl a^2+b^2 ausser durch die genannten Faktoren durch keine andere Zahl, folglich überhaupt durch keine reelle Zahl theilbar. Demnach ist a^2+b^2 eine reelle Primzahl. Ausserdem ist a^2+b^2 von der Form $4n+1$, da von a und b die Eine paar, die andere unpaar ist.

IV. Wenn $a+bi$ eine zusammengesetzte Zahl ist, also als ein Produkt $(a_1+b_1i)(a_2+b_2i)$ dargestellt werden kann; so besteht die Zahl $b+ai$ nach dem vorhergehenden Paragraphen aus den Faktoren (b_1+a_1i), (b_2+a_2i) und i^3, indem man hat $(b+ai) = i^3(b_1+a_1i)(b_2+a_2i)$. Hiernach ist

$$(a+bi)(b+ai) = i^3(a_1+b_1i)(b_1+a_1i)(a_2+b_2i)(b_2+a_2i)$$

oder

$$(a^2+b^2) = (a_1^2+b_1^2)(a_2^2+b_2^2)$$

Folglich ist bei einer zusammengesetzten Zahl die reelle Grösse a^2+b^2 das Produkt aus $a_1^2+b_1^2$ und $a_2^2+b_2^2$, mithin keine reelle Primzahl.

V. Wenn p irgend eine reelle Primzahl von der Form $4n+1$ ist; so lässt sich dieselbe nach §. 156 als die Summe zweier Quadrate a^2+b^2 und zwar nur auf eine einzige Weise darstellen. Diese Summe, nachdem dieselbe mit i multiplizirt ist, kann in die Form des Produktes $(a+bi)(b+ai)$ gebracht werden. Demnach kann p keine vollkommene Primzahl sein.

Da eine solche Zerlegung von p in zwei Quadrate nur in einziger Weise möglich ist; so kann p auch nicht in einer anderen, als der vorstehenden Weise in zwei Faktoren zerlegt werden. Denn wäre auch $p = (a_1+b_1i)(a_2+b_2i)$; so müsste man nach dem vorstehenden Satze IV., da $p = p+0i$ ist,

$$p^2 = (a_1^2+b_1^2)(a_2^2+b_2^2)$$

haben. Dies setzt aber, da p eine reelle Primzahl ist, voraus, dass $a_1^2+b_1^2 = a_2^2+b_2^2 = p$, oder weil p nur auf eine einzige Weise in zwei Quadrate zerlegt werden kann, dass $a_1 = a_2$ und $b_1 = b_2$ oder dass $a_1 = b_2$ und $b_1 = a_2$ sei, was immer nur die einzige Zerlegung $(a+bi)(b+ai)$ herbeiführt.

Hieraus folgt, dass die beiden Faktoren $a+bi$ und $b+ai$ der reellen Primzahl p von der Form $4n+1$ vollkommene Primzahlen sind.

II. Wenn in der vollkommenen Primzahl $a+bi$ die Grösse $b=0$, also jene Primzahl reell ist; so muss sie nach Vorstehendem nothwendig von der Form $4n+3$ sein, da

die reellen Primzahlen von der Form $4n+1$ keine vollkommenen Primzahlen sind. Die Norm a^2+b^2 wird alsdann für eine solche Zahl $=a^2=(4n+3)^2$, also das Quadrat von einer reellen Primzahl der Form $4n+3$ sein.

Umgekehrt ist aber auch jede reelle Primzahl a von der Form $4n+3$ eine vollkommene Primzahl. Denn bestände sie aus den beiden Faktoren $(a_1+b_1i)(a_2+b_2i)$; so müsste nach dem obigen Satze IV.

$$a^2=(a_1^2+b_1^2)(a_2^2+b_2^2)$$

und da a eine reelle Primzahl ist, müsste $a_1^2+b_1^2=a_2^2+b_2^2$ $=a=4n+3$ sein, was nach §. 156 unmöglich ist.

VII. Die vorstehenden Sätze gewähren ein Mittel, aus den reellen Primzahlen alle vollkommenen Primzahlen zu finden. Ausser den reellen Primzahlen von der Form $4n+3$ und der komplexen Zahl $1+i$ gibt es nur noch vollkommene Primzahlen von komplexer Form, welche man erhält, indem man die reellen Primzahlen von der Form $4n+1$ in zwei Quadrate a^2+b^2 zerlegt und daraus die komplexen Zahlen $a+bi$ bildet.

VIII. Was also die Anzahl aller vollkommenen Primzahlen betrifft, deren Norm a^2+b^2 einen gewissen Betrag p nicht übersteigt; so ist dieselbe folgendermaassen zu bestimmen.

Hierbei wollen wir nur diejenigen Zahlen $a+bi$ berücksichtigen, worin weder a, noch b negativ ist, indem $a-bi$, $-a+bi$, $-a-bi$ Produkte der ersteren in eine gewisse Potenz von i sind. Wir wollen aber $a+bi$ und $b+ai$ als zwei verschiedene Primzahlen ansehen, da dieselben nicht bloss durch den Faktor i^r voneinander verschieden sind.

Indessen soll von zwei Zahlen wie $a+0i$ und $0+ai$ nur der Eine, nämlich die reelle Zahl a, mitgezählt werden, da die andere durch Multiplikation mit i aus der ersteren entsteht.

Jetzt hat man

1) die reelle vollkommene Primzahl 1.
2) Die komplexe vollkommene Primzahl $1+i$, für welche $a+bi=b+ai$ und $a^2+b^2=2$ ist.
3) Als reelle vollkommene Primzahlen alle reellen Primzahlen von der Form $4n+3$, welche $\leqq \sqrt{p}$ sind; ihre Anzahl sei $=v$.
4) Als komplexe vollkommene Primzahlen, für welche $a>b$ ist, so viele, als es reelle Primzahlen von der Form $4n+1$ gibt, welche $\leqq p$ sind. Ihre Anzahl sei $=w$.
5) Als komplexe vollkommene Primzahlen, für welche $a<b$ ist, ebenso viele, also w.

Die Gesammtzahl aller dieser vollkommenen Primzahlen ist $2+v+2w$.

So hat man z. B. für $p=100$, also $\sqrt{p}=10$, wegen der reellen vollkommenen Primzahlen 3 und 7 von der Form $4n+3$, welche $\leqq 10$ sind, $v=2$. Ferner, weil es 11 reelle Primzahlen, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, von der Form $4n+1$ gibt, welche $\leqq 100$ sind, $w=11$. Hiernach gibt es $2+2+2.11=26$ vollkommene Primzahlen, deren absoluter Werth <10 ist.

IX. Alle vollkommenen Primzahlen sind unvollkommen paar oder unpaar, mit Ausnahme der Zahl $1+i$, welche vollkommen unpaar ist.

In einer vollkommenen Primzahl $a+bi$ sind ferner a und b vollkommen relativ prim, mit Ausnahme von $1+i$, worin $a=b=1$ ist. Denn besässen sie das gemeinschaftliche Maass m; so wäre m ein Faktor von $a+bi$, mithin die letztere Zahl nicht vollkommen prim.

Auch sind die beiden Werthe $a+b$ und $a-b$ vollkommen relativ prim, mit Ausnahme von $1+i$, worin $a+b=2$ und $a-b=0$ ist. Denn wäre $a+b=mp$ und $a-b=mq$; so hätte man

$$a=\frac{m(p+q)}{2},\qquad b=\frac{m(p-q)}{2}\qquad \text{also}$$

$$a+bi=\frac{m(p+q)}{2}+\frac{m(p-q)}{2}i$$

Wäre nun m nicht $=2$ oder $=2i^r$; so müsste, da $2=i^3(1+i)^2$ ist, selbst wenn m durch $1+i$ theilbar wäre, $a+bi$ den Faktor $1+i$ besitzen, was der Voraussetzung widerspricht.

Wäre aber $m=2$ oder $=2i^r$; so hätte man

$$a+bi=i^r[(p+q)+(p-q)i]$$

und wenn man allgemein $p=p'+p''i$, $q=q'+q''i$ setzt,

$$a+bi=i^r\left\{p'+q''+q'-p''+[p'+q''-(q'-p'')]i\right\}$$

folglich

$$a^2+b^2=2[(p'+q'')^2+(q'-p'')^2]$$

was unmöglich ist, da a^2+b^2 eine reelle Primzahl ist.

Aus dem letzten Satze folgt, dass wenn $a+b$ und $a-b$ kein gemeinschaftliches Maass haben, ihr Produkt, also die Grösse a^2-b^2, keinen reellen oder komplexen quadratischen Faktor haben kann.

§. 195. **Praktisches Verfahren behuf Zerlegung einer Zahl in ihre vollkommenen Primfaktoren.**

I. Der Besitz einer Tafel der reellen Primzahlen genügt, um nach dem vorhergehenden Paragraphen die sukzessiv aufsteigenden vollkommenen Primzahlen zu bestimmen.

Eine solche Tafel genügt aber auch, um jede gegebene reelle oder komplexe Zahl in ihre vollkommenen Primfaktoren zu zerlegen. Man kann zu diesem Ende folgendermaassen operiren.

Wenn $A+Bi$ die zu zerlegende Zahl ist; so ermittelt man zuerst das grösste gemeinschaftliche reelle Maass der beiden reellen Zahlen A und B, sondert dasselbe ab und zerlegt es in seine reellen Primfaktoren. Dies ergebe

(1) $$A+Bi=(p^\alpha q^\beta\ldots)(A'+B'i)$$

Alle diejenigen der reellen Faktoren p, $q\ldots$, welche die Form $4n+3$ besitzen, sind vollkommene Primzahlen. Jeder andere dieser reellen Faktoren liefert, wenn er $=2$ ist, die Zerlegung $2=i^3(1+i)^2$, und wenn er von der Form $4n+1$ ist, indem man denselben in zwei Quadrate a^2+b^2 zerfällt, die Zerlegung $i^3(a+bi)(b+ai)$, worin $a+bi$ und $b+ai$ vollkommen prim sein werden.

II. Was den komplexen Faktor $A'+B'i$ betrifft; so hat man zunächst, wenn A' und B' beide unpaar sind, $1+i$ als Faktor abzusondern. Dies gibt

(2) $$A'+B'i=(1+i)\frac{A'+B'i}{1+i}=(1+i)\left(\frac{A'+B'}{2}+\frac{B'-A'}{2}i\right)$$
$$=(1+i)(A''+B''i)$$

worin nun von A'' und B'' die Eine paar, die andere unpaar sein wird.

III. Wäre jedoch schon in $A'+B'i$ von den beiden Zahlen A' und B' die Eine paar, die andere unpaar; so behandelt man diesen Faktor nach folgender Regel, welche eventuell auch auf den Faktor $A''+B''i$ Anwendung findet.

Man stelle sich vor, es sei

(3) $$A'+B'i=i^m(a_1+b_1i)(a_2+b_2i)\ldots(a_n+b_ni)$$

worin a_1+b_1i, a_2+b_2i u. s. w. vollkommene Primzahlen darstellen, von denen auch mehrere einander gleich sein können. Alsdann ist nach §. 193, III.

(4) $$B'+A'i=i^{3(m+n-1)}(b_1+a_1i)(b_2+a_2i)\ldots(b_n+a_ni)$$

folglich

(5) $$(A'+B'i)(B'+A'i)i^3=A'^2+B'^2=(a_1^2+b_1^2)(a_2^2+b_2^2)\ldots$$
$$\ldots(a_n^2+b_n^2)$$

Hiernach bildet man aus dem Faktor $A' + B'i$ die Grösse $A'^2 + B'^2$ und zerlegt dieselbe in ihre reellen Primfaktoren, welche sämmtlich von der Form $4r + 1$ sein werden und die Stelle der Grössen $a_1^2 + b_1^2$, $a_2^2 + b_2^2, \ldots$ vertreten.

Aus dem ersten Faktor $a_1^2 + b_1^2$ stellt man die beiden vollkommenen Primzahlen $a_1 + b_1 i$ und $b_1 + a_1 i$ her. Die Zahl $A' + B'i$ ist nun entweder durch $a_1 + b_1 i$ oder durch $b_1 + a_1 i$ theilbar. Man untersucht also, ob

$$(6) \qquad \frac{A' + B'i}{a_1 + b_1 i} = A'' + B''i$$

eine ganze Zahl sei. Findet sich Dies nicht bestätigt; so muss nothwendig

$$(7) \qquad \frac{A' + B'i}{b_1 + a_1 i} = A'' + B''i$$

eine ganze Zahl sein.

Nachdem hierdurch entweder $a_1 + b_1 i$ oder $b_1 + a_1 i$ als Faktor von $A' + B'i$ gefunden ist, fährt man in derselben Weise fort, den Quotienten $A'' + B''i$, für welchen man

$$A''^2 + B''^2 = (a_2^2 + b_2^2) \ldots (a_n^2 + b_n^2)$$

hat, zu zerlegen, wodurch sich zunächst entweder der Faktor $a_2 + b_2 i$ oder $b_2 + a_2 i$ ergibt.

Der letzte Quotient muss die zuletzt in Betracht kommende Primzahl $a_n + b_n i$ oder $b_n + a_n i$ selbst sein.

Es wird noch bemerkt, dass wenn mehrere der Grössen $a_1^2 + b_1^2$, $a_2^2 + b_2^2 \ldots$ einander gleich wären, wenn man also $(a_1^2 + b_1^2)(a_2^2 + b_2^2) \ldots (a_r^2 + b_r^2) = (a_1^2 + b_1^2)^r$ hätte, $A' + B'i$ entweder nur durch $(a_1 + b_1 i)^r$ oder durch $(b_1 + a_1 i)^r$, nicht aber gleichzeitig durch $a_1 + b_1 i$ und $b_1 + a_1 i$ theilbar ist. Denn wäre das Letztere der Fall; so müsste jene Zahl auch durch $(a_1 + b_1 i)(b_1 + a_1 i) = (a_1^2 + b_1^2)i$, also auch durch die reelle Zahl $a_1^2 + b_1^2$ theilbar sein, was der Voraussetzung widerspricht, indem $A' + B'i$ bereits von allen reellen Faktoren befreiet ist.

IV. Beispiel. Es sei $29 + 3i$ zu zerlegen. Da 29 und 3 relativ prim sind; so hat jene Zahl keinen reellen Faktor. Da dieselbe aber vollkommen unpaar ist; so hat sie den Faktor $1 + i$, und es findet sich $\frac{29 + 3i}{1 + i} = 16 - 13i$.

Um jetzt $16 - 13i$ zu zerlegen, hat man $16^2 + 13^2 = 425 = 5^2 . 17 = (2^2 + 1^2)^2(4^2 + 1^2)$. Da man findet, dass $16 - 13i$ nicht durch $2 + i$ theilbar ist; so muss sie durch $1 + 2i$ und

zwar durch $(1+2i)^2$ theilbar sein. In der That ist $\frac{16-13i}{(1-2i)^2}$ $= -4-i$, und es ist klar, dass dieser letzte Quotient $-4-i$ zugleich der letzte vollkommene Primfaktor ist.

Hiernach hat man folgende Zerlegung

$$29+3i = i^2(1+i)(1+2i)^2(4+i)$$

§. 196. *Kettenbrüche mit komplexen Quotienten und Entwickelung eines komplexen Bruches in einen Kettenbruch.*

I. Denken wir uns jetzt an die Stelle der reellen Quotienten der im ersten Abschnitte betrachteten Kettenbrüche komplexe Zahlen gesetzt; so entstehen, wenn das Additionsprinzip zu Grunde liegt, Kettenbrüche von der allgemeinen Form

$$K = a_0+b_0i+\cfrac{1}{a_1+b_1i+\cfrac{1}{a_2+b_2i+\text{etc.}}} = [a_0+b_0i,\ a_1+b_1i,\ a_2+b_2i\ldots]$$

II. Die Reduktion eines solchen Kettenbruches auf einen gewöhnlichen Bruch geschieht genau nach den früheren Prinzipien und kann demnach auch nach demselben Schema ausgeführt werden. So hat man z. B. für den Kettenbruch

$$3+\cfrac{1}{2i+\cfrac{1}{3+\cfrac{1}{1+2i}}} = [3,\ 2i,\ 3,\ 1+2i]$$

die Reduktion

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	3	3	1
1	$2i$	$1+bi$	$2i$
2	3	$6+18i$	$1+6i$
3	$1+2i$	$-29+36i$	$-11+10i$

Jener Kettenbruch ist also gleich $\frac{-29+36i}{-11+10i}$.

III. Für die beiden Grössen N_{-2} und M_{-1}, welche gewöhnlich $=1$ gesetzt werden, kann man bekanntlich, wenn es sich nur um reelle Zahlen handelt, auch -1 setzen, wodurch sich die Zeichen der Zähler und Nenner aller Näherungsbrüche in die entgegengesetzten verwandeln.

Hier, wo auch imaginäre Zahlen für zulässig erachtet werden, kann man für jene beiden Grössen jede beliebige

Potenz von i setzen, was immer nur einen gleichmässigen Einfluss auf das Richtungszeichen der Zähler und Nenner aller Näherungsbrüche ausübt.

So könnte man im vorigen Beispiele auch folgende Reduktion bilden, wobei $N_{-2} = M_{-1} = i$ genommen ist.

n	a_n	M_n	N_n
-2		0	i
-1		i	0
0	3	$3i$	i
1	$2i$	$-6+i$	-2
2	3	$-18+6i$	$-6+i$
3	$1+2i$	$-36-29i$	$-10-11i$

IV. Kettenbrüche mit komplexen Quotienten entstehen unvermeidlich bei der Entwickelung eines gewöhnlichen Bruches mit komplexem Zähler oder Nenner. Aus der Natur der Kettenbrüche erhellet, dass man zur Ermittelung der Quotienten eines Kettenbruches, welcher einem gewöhnlichen Bruche gleich sein soll, genau dieselbe Rechnung zu vollführen hat, welche in §. 191 zur Aufsuchung des grössten gemeinschaftlichen Maasses zwischen dem Zähler und Nenner des letzteren Bruches angegeben ist. Bei dieser Rechnung sind immer Divisionen mit absolut kleinsten Resten vorzunehmen, was eine fortwährende Verkleinerung der Reste oder Divisoren und demnach einen Schluss der Rechnung nach endlicher Gliederzahl zur Folge hat.

So ist z. B. im Beispiele 1. des §. 191 die Kettenbruchsentwickelung von $\frac{35+6i}{3+28i}$ dargestellt. Man hat dafür $[-i,\ 3+i,\ 1-3i]$. Eine Reduktion dieses Kettenbruches ergibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	$-i$	$-i$	1
1	$2+i$	$2-2i$	$2+i$
2	$1-3i$	$-4-9i$	$6-5i$

also den Bruch $\frac{-4-9i}{6+5i}$. Dieser Bruch ist dem gegebenen $\frac{35+6i}{3+28i}$ gleich, da Zähler und Nenner des letzteren das gemeinschaftliche Maass $-2+3i$ besitzen.

V. Es leuchtet ein, dass man in jede Kettenbruchsentwickelung auch ganz willkürliche komplexe Quotienten einfüh-

ren, von jeder beliebigen späteren Stelle an aber die Entwickelung zum Schlusse führen kann, indem man fortan nur Divisionen mit absolut kleinsten Resten ausführt.

§. 197. Werthverhältniss der Näherungsbrüche einer Kettenbruchsentwickelung mit absolut kleinsten Resten.

I. Die Berechnung der Quotienten $a_0 + b_0 i$, $a_1 + b_1 i$, $a_2 + b_2 i$ etc., welche bei der Entwickelung eines Bruches

(1)
$$K = \frac{M}{N} = \frac{A + Bi}{A_1 + B_1 i}$$

in einen Kettenbruch mit absolut kleinsten Resten entstehen, wird nach dem Vorstehenden und nach §. 190, I. und IV. in folgender Weise ausgeführt. Man setzt zunächst

(2)
$$\frac{A + Bi}{A_1 + B_1 i} = \frac{(AA_1 + BB_1) + (BA_1 - AB_1)i}{A_1^2 + B_1^2}$$
$$= a_0 + b_0 i + \frac{r + si}{A_1^2 + B_1^2}$$

worin numerisch

(3) r und $s \leqq \frac{1}{2}(A_1^2 + B_1^2)$, also $r^2 + s^2 \leqq \frac{1}{2}(A_1^2 + B_1^2)^2$

oder worin der absolute Werth des reellen und des imaginären Theiles des Restes, d. i. $\frac{r}{A_1^2 + B_1^2}$ und $\frac{s}{A_1^2 + B_1^2} \leqq \frac{1}{2}$, also die Norm des Restes oder $\frac{r^2 + s^2}{(A_1^2 + B_1^2)^2} < \frac{1}{2}$, mithin der absolute Werth dieses Restes $< \frac{1}{\sqrt{2}}$ oder $< \frac{1}{2}\sqrt{2}$ ist. Hierauf bildet man

(4)
$$\frac{A + Bi}{A_1 + B_1 i} = a_0 + b_0 i + \frac{R + Si}{A_1 + B_1 i}$$

worin

(5)
$$R = \frac{A_1 r - B_1 s}{A_1^2 + B_1^2}, \qquad S = \frac{B_1 r + A_1 s}{A_1^2 + B_1^2}$$

ist. Nachdem auf diese Weise der erste Quotient $a_0 + b_0 i$ und der erste Rest $R + Si$ gefunden ist, führt eine ähnliche Rechnung zu dem zweiten Quotienten $a_1 + b_1 i$ und zu dem zweiten Reste $R_1 + S_1 i$, indem man $R + Si$ zum Divisor und $A_1 + B_1 i$ zum Dividende nimmt, also die Formel

(6)
$$\frac{A_1 + B_1 i}{R + Si} = a_1 + b_1 i + \frac{r_1 + s_1 i}{R^2 + S^2} = a_1 + b_1 i + \frac{R_1 + S_1 i}{R + Si}$$

in der obigen Weise berechnet.

Statt dieser zweiten zur Ermittelung des zweiten Quotienten $a_1 + b_1 i$ dienenden Rechnung, welche sich auf die Entwickelung des umgekehrten Werthes $\frac{A_1 + B_1 i}{R + Si}$ des zweiten Gliedes der rechten Seite der Gl. (4) stützt, kann man auch das gleichbedeutende Glied $\frac{r + si}{A_1^2 + B_1^2}$ aus Gl. (2) umkehren und die hieraus entstehende Grösse $\frac{A_1^2 + B_1^2}{r + si}$ entwickeln. Dies gibt

(7) $$\frac{A_1^2 + B_1^2}{r + si} = \frac{(A_1^2 + B_1^2)r - (A_1^2 + B_1^2)si}{r^2 + s^2}$$

und es ist nun

(8) $$a_1 \text{ aus } \frac{(A_1^2 + B_1^2)r}{r^2 + s^2}$$

(9) $$b_1 \text{ aus } -\frac{(A_1^2 + B_1^2)s}{r^2 + s^2}$$

nach dem Prinzipe des absolut kleinsten Restes zu bestimmen.

II. Um die unteren Gränzen zu bestimmen, oberhalb welcher die absoluten Werthe von a_1 und b_1 jedenfalls liegen müssen, ist klar, dass wenn der absolute Werth des Bruches, aus welchem a_1 zu bestimmen ist, $=$ einer ganzen Zahl n ist, auch der numerische Werth von $a_1 = n$ ist, dass dagegen, wenn jener Bruch $> n$ ist, $a_1 \geqq n$ sein wird, ferner, dass wenn jener Bruch $= n + \frac{1}{2}$ ist, a_1 sowol $= n$, als auch $= n + 1$ genommen werden kann, endlich, dass wenn jener Bruch $> n + \frac{1}{2}$ ist, $a_1 \geqq n + 1$ sein wird.

Suchen wir nun die unteren Gränzwerthe der obigen beiden Brüche, aus denen a_1 und b_1 bestimmt werden muss, zu ermitteln. Da wegen der Beziehungen (3) numerisch $A_1^2 + B_1^2 \geqq 2r$ und auch $\geqq 2s$ ist; so hat man

(10) $$\frac{(A_1^2 + B_1^2)r}{r^2 + s^2} \geqq \frac{2r^2}{r^2 + s^2}$$

(11) $$\frac{(A_1^2 + B_1^2)s}{r^2 + s^2} \geqq \frac{2s^2}{r^2 + s^2}$$

Von den beiden Brüchen $\frac{2r^2}{r^2 + s^2}$ und $\frac{2s^2}{r^2 + s^2}$ kann keiner $= \frac{1}{2}$ auch nicht $= \frac{3}{2}$ sein. Denn wäre z. B. $\frac{2r^2}{r^2 + s^2} = \frac{1}{2}$;

so müsste $s^2 = 3r^2$ oder $s = r\sqrt{3}$ sein, was unmöglich ist, weil s und r ganze Zahlen sind. Es kann also nur sein

$$\frac{2r^2}{r^2+s^2} \gtrless \frac{1}{2}, \text{ und hieraus folgt } \frac{2s^2}{r^2+s^2} \lessgtr \frac{3}{2}$$

oder es kann sein

$$\frac{2r^2}{r^2+s^2} \gtrless \frac{3}{2}, \text{ und hieraus folgt } \frac{2s^2}{r^2+s^2} \lessgtr \frac{1}{2}$$

worin gleichzeitig die oberen oder die unteren Zeichen zu nehmen sind. Berücksichtigt man hierbei noch, dass wenn

$$\frac{2r^2}{r^2+s^2} \underset{\leqq}{>} 1 \text{ ist, } \frac{2s^2}{r^2+s^2} \underset{\geqq}{<} 1 \text{ sein wird;}$$

so ist leicht zu erachten, dass die kleinsten Werthe von a_1 und b_1 sich nur in folgender Weise kombiniren können.

$$a_1 = 1, \quad 2, \quad 0$$
$$b_1 = 1, \quad 0 \quad 2$$

Demnach ist

(12) $$a_1^2 + b_1^2 \geqq 2$$

Dieses ist das Minimum der Norm nicht bloss für den zweiten Quotienten vom Zeiger 1, sondern auch für jeden späteren. Nur für den ersten Quotienten vom Zeiger 0 ist es möglich, dass man $a_0^2 + b_0^2 = 1$ oder $= 0$ habe.

Hätte man es mit lauter reellen Zahlen zu thun; so müsste wegen der Beziehungen (12) die Norm eines jeden Quotienten von a_1 an $\geqq 2$, also sein absoluter Werth selbst > 1, folglich $\geqq 2$ sein, wie auch bereits in §. 22 gefunden ist.

III. Wenn unter den Quotienten von $a_1 + b_1 i$ an keiner der Werthe $1 + i$ oder $-1 + i$, deren Norm $= 2$ ist, sondern nur solche vorkommen, deren Norm > 2, also $\geqq 4$ oder deren absoluter Werth $\geqq 2$ ist; so kann man leicht zeigen, dass die Normen der Zähler und Nenner der Näherungsbrüche sukzessiv wachsen.

Denn schreibt man, um die Formeln abzukürzen, einen komplexen Ausdruck wie $a + bi$ in der Form $re^{\varphi i}$, worin $r = \sqrt{a^2+b^2}$ der absolute Werth, $r^2 = a^2 + b^2$ die Norm, $\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}$ und $\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}$ ist; so sei der Zähler oder Nenner irgend eines Näherungsbruches vom Zeiger $n-2$ gleich $re^{\varphi i}$ und der nächstfolgende vom Zeiger $n-1$ gleich $r_1 e^{\varphi_1 i}$, ferner der Quotient vom Zeiger n gleich $ae^{\alpha i}$. Für den Zähler oder Nenner vom Zeiger n würde man alsdann haben

$$r_2 e^{\varphi_2 i} = ae^{\alpha i} r_1 e^{\varphi_1 i} + re^{\varphi i} = ar_1 e^{(\alpha+\varphi_1 i)} + re^{\varphi i}$$
$$= [ar_1 \cos(\alpha+\varphi_1) + r\cos\varphi] + [ar_1 \sin(\alpha+\varphi_1) + r\sin\varphi]i$$

Folglich ist der absolute Werth r_2 dieser Grösse

$$r_2 = \sqrt{[ar_1 \cos(\alpha + \varphi_1) + r \cos\varphi]^2 + [ar_1 \sin(\alpha + \varphi_1) + r \sin\varphi]^2}$$
$$= \sqrt{a^2r_1^2 + 2arr_1 \cos(\alpha + \varphi_1 - \varphi) + r^2}$$

Der kleinste Werth, welchen dieser Ausdruck möglicher Weise annehmen kann, ist der, für welchen numerisch $\cos(\alpha + \varphi_1 - \varphi) = 1$ und das darin multiplizirte Glied negativ wird. Alsdann hat man aber, indem a, r, r_1 nur absolute Werthe darstellen,

$$r_2 = ar_1 - r$$

Ist nun $r_1 \geqq r$ und der absolute Werth $a \geqq 2$; so ist offenbar $r_2 \geqq r_1$, und zwar ist die Gleichheit $r_2 = r_1$ nur in dem besonderen Falle denkbar, wo auf Ein Mal $r_1 = r$ und $a = 2$ ist. Es werden also unter diesen Umständen die absoluten Werthe der Zähler und Nenner der Näherungsbrüche, folglich auch ihre Normen allmählig wachsen, oder doch auf keinen Fall sich verkleinern.

IV. Es leuchtet ein, dass für die Kettenbrüche mit komplexen Quotienten, gleichviel, ob die Entwickelung mit kleinsten Resten geschehen ist oder nicht, die Formeln der §§. 4 und 6 unter angemessener Modifikation der Begriffe hinsichtlich der Fehlergränze Gültigkeit besitzen, insofern man für die Grössen M_{-1} und N_{-2} entweder den Werth 1 oder -1 angenommen hat. Demnach hat man allgemein

$$M_nN_{n-1} - M_{n-1}N_n = (-1)^{n-1} \tag{13}$$

worin M und N die komplexen Zähler und Nenner von Näherungsbrüchen darstellen. So hat man z. B. für den im vorhergehenden Paragraphen sub IV. entwickelten Kettenbruch

$$M_2N_1 - M_1N_2 = (-1)^1 = -1$$

nämlich

$$(-4 + 9i)(2 + i) - (2 - 2i)(6 - 5i) = -1$$

Hätte man jedoch für M_{-1} und N_{-2} entweder den Werth i oder $-i$ angenommen, so würde statt Gl. (13)

$$M_nN_{n-1} - M_{n-1}N_n = (-1)^n \tag{14}$$

V. Ebenso hat man für die Differenz zweier benachbarten Näherungsbrüche K_n und K_{n+1}, jenachdem die Gl. (13) oder (14) gilt, resp.

$$K_{n+1} - K_n \text{ entweder } = \frac{(-1)^n}{N_nN_{n+1}} \text{ oder } = \frac{(-1)^{n+1}}{N_nN_{n+1}} \tag{15}$$

und als Werthverhältniss der Differenzen zwischen dem Gesammtwerthe K des ganzen Kettenbruches und den Näherungsbrüchen K_n und K_{n+1} in beiden Fällen

$$\frac{K - K_{n+1}}{K - K_n} = -\frac{N_nx_{n+1}}{N_{n+1}} \tag{16}$$

so müsste $s^2 = 3r^2$ oder $s = r\sqrt{3}$ sein, was ... eichnet.
s und r ganze Zahlen sind. Es kann also ... etc.

$$\frac{2r^2}{r^2+s^2} \gtrless \frac{1}{2},$$ und hieraus fol... denjenigen ... er der Nähe-

oder es kann sein ... auch stets die

$$\frac{2r^2}{r^2+s^2} \gtrless \frac{3}{2},$$ und hier... $\leqq \sqrt{\frac{1}{2}}$, folg-

worin gleichzeitig die ober... wickelung mit ab-
nehmen sind. Berücksichti... die Normen der

$$\frac{2r^2}{r^2+s^2} \gtrless 1$$ ... zwei benachbarten ... zwischen dem Ge-

so ist leicht zu era... ...es und den sukzessiv
b_1 sich nur in fol... ...n allmählig kleiner wer-
...esetz stattfinde, ist es übrigens nicht
...u, dass die Nenner der Näherungsbrüche
Demnach i... wachsen, oder dass stets $N_{n+1} > N_n$ sei. Es braucht
(12) ... der absolute Werth oder die Norm von $\frac{N_{n+1}}{x_{n+1}} > N_n$
Di...
zwei... was schon dann der Fall ist, wenn man $\sqrt{2}\, N_{n+1} > N_n$
te...
r... Setzt man $N_n = re^{\varphi i}$, $N_{n+1} = r_1 e^{\varphi_1 i}$, $x_{n+1} = xe^{\psi i}$; so nimmt die Formel (15), jenachdem Gl. (13) oder (14) gilt, resp. die Gestalt

$$(17)\quad K_{n+1} - K_n \text{ entweder } = \frac{(-1)^n}{rr_1 e^{(\varphi+\varphi_1)i}} = \frac{(-1)^n}{rr_1} e^{-(\varphi+\varphi_1)i}$$

$$= \frac{(-1)^n}{rr_1} cos(\varphi+\varphi_1) - \frac{(-1)^n}{rr_1} sin(\varphi+\varphi_1).i$$

$$\text{oder } = \frac{(-1)^{n+1}}{rr_1} cos(\varphi+\varphi_1) - \frac{(-1)^{n+1}}{rr_1} sin(\varphi+\varphi_1)i$$

und die Formel (15) die Gestalt

$$(18)\quad \frac{K - K_{n+1}}{K - K_n} = -\frac{re^{\varphi i} xe^{\psi i}}{r_1 e^{\varphi_1 i}} = -\frac{rx}{r_1} e^{(\varphi+\psi-\varphi_1)i}$$

$$= -\frac{rx}{r_1} cos(\varphi+\psi-\varphi_1) - \frac{rx}{r_1} sin(\varphi+\psi-\varphi_1).i$$

an. Beachtet man, dass unter den zuletzt erwähnten Voraussetzungen die Grössen $\frac{1}{rr_1}$ und $\frac{rx}{r_1}$ sukzessiv abnehmen, und dass die Sinus und Kosinus den Werth 1 nicht übersteigen können; so erkennt man aus diesen Formeln, dass die vorhin bezeichnete allmählige Verringerung der Differenzen sich nicht bloss auf die numerischen Werthe oder Normen der kom-

plexen Grössen, welche diese Differenzen darstellen, sondern auch auf die absoluten Werthe der reellen und der imaginären Theile jener komplexen Differenzen für sich allein genommen erstrecken. In Beziehung auf die zuletzt genannten Differenzen kann das fragliche Gesetz übrigens ein wenig durch die Schwankungen der Sinus und Kosinus gestört werden, und, streng genommen, kann man nur sagen, dass die möglichen Maxima dieser Differenzen sich fortwährend vermindern.

VI. Als Beispiel zu den vorstehenden Sätzen diene folgende Entwickelung des Bruches

$$\frac{75-288i}{167+7i}=\frac{10509}{27938}-\frac{48621}{27938}i.$$

n	a_n	M_n	N_n	K_n
-2		0	1	
-1		1	0	
0	$-2i$	$-2i$	1	$\frac{-2i}{1} = -2i$
1	$2-i$	$-1-4i$	$2-i$	$\frac{-1-4i}{2-i} = \frac{2}{5}-\frac{9}{5}i$
2	$-2+2i$	$10+4i$	$-1+6i$	$\frac{10+4i}{-1+6i} = \frac{14}{37}-\frac{64}{37}i$
3	$-2i$	$7-24i$	$14+i$	$\frac{7-24i}{14+i} = \frac{74}{197}-\frac{343}{197}i$
4	$-2+4i$	$92+80i$	$-33+60i$	$\frac{92+80i}{-33+60i} = \frac{1764}{4689}-\frac{8160}{4689}i$
5	$-1-2i$	$75-288i$	$167+7i$	$\frac{75-288i}{167+7i} = \frac{10509}{27938}-\frac{48621}{27938}i$

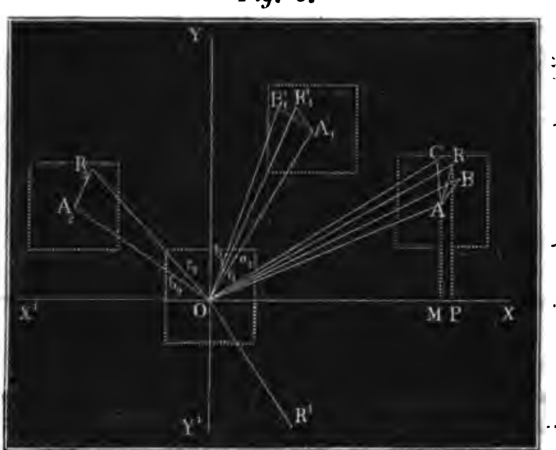
§. 198. ***Vervollständigung der Gesetze des vorhergehenden Paragraphen für den Fall, dass Quotienten von der Form*** **($\pm 1 \pm$ i)** ***vorkommen. — Geometrisches Bild einer Kettenbruchsentwickelung in komplexen Zahlen.***

I. Es bleibt noch der im vorhergehenden Paragraphen ausgeschlossene Fall zu betrachten, wo unter den Quotienten der Kettenbruchsentwickelung von K vom zweiten Quotienten an auch Werthe von der Form $(\pm 1 \pm i)$ vorkommen. In diesem Falle kann man behaupten, dass die absoluten Werthe oder Normen der Zähler und Nenner der Näherungsbrüche K_n ununterbrochen wachsen, auch dass die vollständigen Werthe dieser Brüche sich dem Werthe von K nähern, also die absoluten Werthe oder Normen der Differenz $K-K_n$ sich vermindern, insofern

man in diesen Reihen unter Umständen gewisse einzelne Glieder als Abnormitäten ausscheidet.

Zum Beweise dieses wichtigen Satzes erlaube ich mir, in das Gebiet der geometrischen Anschauung überzutreten. Obgleich eine rein arithmetische Rechnung schliesslich dasselbe Resultat liefern würde, und es im Ganzen wol angemessen wäre, hier bei der abstrakten Auffassung zu beharren; so zweifele ich doch nicht, dass die Eigenthümlichkeit der nachfolgenden Untersuchung, namentlich aber die Klarheit, welche die geometrische Konstruktion dem zu erläuternden, ziemlich komplizirten analytischen Gesetze mit seinen vielen beachtenswerthen Nebenbeziehungen verleihet, sowie der Nachweis, dass sich die Prinzipien des Situationskalkuls(*) mit Vortheil und Eleganz sogar auf die schwierigeren Untersuchungen über diskrete Grössen, nämlich hier über ganze Zahlen, übertragen lassen, das Interesse manches Lesers in Anspruch nehmen werde.

Fig. 6.



In Fig. (6) sei O der Nullpunkt, OX die positiv reelle und OY die positiv imaginäre Axe. Es kommt darauf an, eine Grösse $K = \frac{A + Bi}{A_1 + B_1 i}$, welche nach einer bekannten Umwandlung in der Form

$$(1) \qquad K = a + bi = re^{\varphi i}$$

dargestellt sei, in einen Kettenbruch mit absolut kleinsten Resten zu entwickeln. Die Quotienten desselben seien

(*) Unter diesem Titel in einer besonderen Schrift des Verfassers vom Jahre 1851 ausführlich entwickelt.

(2) $a_0 + b_0 i = r_0 e^{\varphi_0 i}$, $a_1 + b_1 i = r_1 e^{\varphi_1 i}$, $a_2 + b_2 i = r_2 e^{\varphi_2 i}$ u. s. w. In allen diesen Ausdrücken können die beiden Zahlen a und b, welche stets ganz sein müssen, sowol positiv, wie negativ sein. Die Zahl r, welche den absoluten Werth der betreffenden komplexen Grösse oder die Länge der korrespondirenden Linie bezeichnet, ist stets positiv und im Allgemeinen irrational, wogegen ihr Quadrat oder die Norm r^2 eine ganze Zahl ist; die Zahl φ stellt einen Winkel dar, dessen positive Drehungsrichtung von OX nach OY oder von rechts nach links herum gedacht wird; dieser Winkel kann positiv und negativ und absolut $\leqq \pi$, oder er kann stets positiv und $\leqq \pi$ genommen werden. Eine nach Länge und Richtung aufgefasste Zahl $re^{\varphi i}$ werden wir zur Abkürzung oftmals mit (r) bezeichnen, indem wir nämlich den Buchstaben r, welcher den absoluten Werth jener Zahl bezeichnet, in Klammern schliessen.

Wenn $OP = a$, $PR = b$, also $OR = r$ und $ROP = \varphi$ ist; so ist die Linie (OR) die in Kettenbruchsform darzustellende.

II. Der erste Quotient, welcher die der Zahl (OR) zunächst liegende ganze Zahl darstellt und gleich dem Näherungsbruche K_0 ist, sei (OA), man habe also

$$(3) \qquad (OA) = a_0 + b_0 i = r_0 e^{\varphi_0 i} = (r_0)$$

Da nach dem Prinzipe der absolut kleinsten Reste verfahren wird; so muss die Länge der Differenz (AR) zwischen (OR) und (OA) oder zwischen (r) und (r_0) bekanntlich $\leqq \frac{1}{\sqrt{2}}$ oder $\leqq \frac{1}{2}\sqrt{2}$, also kleiner als die halbe Diagonale eines mit der Einheit als Seite beschriebenen Quadrates sein, und da ausserdem die Länge sowol des reellen, wie des imaginären Theiles dieses Restes $\leqq \frac{1}{2}$ sein muss (s. §. 197, No. I.); so folgt, dass der Punkt R innerhalb oder im Umfange eines Quadrates liegt, dessen Seite gleich der Einheit, dessen Mittelpunkt A ist und dessen Seitenlinien den Grundaxen parallel sind. Dieses Quadrat, welches wir mit $\square_0$ bezeichnen wollen, ist in der Figur dargestellt. Der Rest (AR) sei

$$(4) \qquad (AR) = c_0 + d_0 i = s_0 e^{\psi_0 i} = (s_0)$$

Jetzt ist zur Bestimmung des zweiten Quotienten (r_1) von dem umgekehrten oder reziproken Werthe des Restes (s_0), also von $\frac{1}{(s_0)}$ nach demselben Prinzipe die zunächst liegende ganze Zahl abzusondern. Es ist aber

$$(5) \qquad \frac{1}{(s_0)} = \frac{1}{s_0 e^{\psi_0 i}} = \frac{1}{(s_0)} e^{-\psi_0 i}$$

Der absolute Werth des Umgekehrten oder der Reziproke von (s_0) ist also das Umgekehrte oder die Reziproke des absoluten Werthes dieser Grösse, nämlich $=\frac{1}{s_0}$, während der Neigungswinkel jener Reziproke, nämlich $-\psi_0$, das dem Zeichen nach Entgegengesetzte des Neigungswinkels jener Grösse ist. Um daher $\frac{1}{(s_0)}$ darzustellen, trägt man (AR) parallel zu sich selbst an den Nullpunkt O, was (Or) ergebe, macht in derselben Richtung $OR_1=\frac{1}{Or}=\frac{1}{s_0}$, nimmt den Winkel XOR' auf der entgegengesetzten Seite der reellen Axe $=XOR_1=\psi_0$ und die Länge von $OR'=OR_1$; alsdann ist $(OR')=\frac{1}{(s_0)}$. Zur leichteren Übersicht wollen wir jedoch, da das ganze Zahlennetz unterhalb der reellen Axe demjenigen oberhalb dieser Axe symmetrisch ist, die Linie (OR_1) in der direkten Richtung von (Or) für die Linie $(OR')=\frac{1}{(s_0)}$ nehmen, indem wir uns, wo es nöthig ist, die Umwälzung der Figur um die reelle Axe in Gedanken vorstellen.

Ist nun (OA_1) die zunächst an (OR_1) liegende ganze Zahl; so hat man

$$(6)\qquad (OA_1)=a_1+b_1 i=r_1 e^{\varphi_1 i}=(r_1)$$

und es liegt der Punkt R_1 in einem dem früheren ähnlichen Quadrate $\square_1$.

Bricht man den Kettenbruch hinter dem zweiten Quotienten (r_1) ab; so stellt sich der zweite Näherungsbruch K_1 folgendermaassen dar. Man nimmt die Reziproke von $(OA_1)=(r_1)$, welche in derselben Richtung liegt und $=(Oa_1)=\frac{1}{(r_1)}$ sei, und trägt hierauf diese Linie parallel zu sich selbst an den Punkt A, sodass $(AB)=(Oa_1)$ ist. Alsdann ist

$$(OB)=(r_0)+\frac{1}{(r_1)}=K_1$$

der zweite Näherungsbruch.

Nach dem weiter unten zu erweisenden Gesetze soll nun (abgesehen von gewissen Ausnahmen) die Differenz zwischen K und K_1 einen kleineren numerischen Werth haben, als die Differenz zwischen K und K_0, d. h. es soll der Punkt B näher an R liegen, als der Punkt A, oder es soll die Linie RB kürzer sein, als die Linie RA.

Zur Ermittelung des dritten Quotienten ist die Differenz oder der Rest

(7) $$(A_1R_1) = c_1 + d_1 i = s_1 e^{\psi_1 i} = (s_1)$$

zwichen (OR_1) und (OA_1) umzukehren, also $\frac{1}{(s_1)}$ zu bilden und daraus die zunächst liegende ganze Zahl zu nehmen. Dies geschieht wie vorhin, indem man (A_1R_1) parallel zu sich selbst an den Nullpunkt nach (Or_2) trägt und in der Richtung dieser Linie $OR_2 = \frac{1}{Or_2} = \frac{1}{s_1}$ macht. Ist dann (OA_2) die zunächst liegende ganze Zahl; so hat man

(8) $$(OA_2) = a_2 + b_2 i = r_2 e^{\varphi_2 i} = (r_2)$$

und es liegt der Punkt R_2 in einem dem früheren ähnlichen Quadrate $\square_2$.

Wird jetzt der Kettenbruch hinter dem dritten Quotienten (r_2) abgebrochen; so findet man den dritten Näherungsbruch K_2 durch folgende Zeichnung, Man nimmt die Reziproke von $(OA_2) = (r_2)$, welche $= (Oa_2) = \frac{1}{(r_2)}$ sei, und trägt diese Linie parallel zu sich selbst an den Punkt A_1, sodass $(A_1B_1) = (Oa_2)$ ist. Zieht man hierauf OB_1; so ist diese Linie $= (OA_1) + (A_1B_1)$ $= (r_1) + \frac{1}{(r_2)}$. Hierauf nimmt man die Reziproke von (OB_1), welche $= (Ob_1)$, also $= \cfrac{1}{(r_1) + \cfrac{1}{(r_2)}}$ sei, und trägt dieselbe parallel zu sich selbst an den Punkt A nach (AC). Zieht man dann OC; so ist

$$(OC) = (r_0) + \cfrac{1}{(r_1) + \cfrac{1}{(r_2)}} = K_2$$

der dritte Näherungsbruch.

Nach dem in Rede stehenden Gesetze muss nun wieder (abgesehen von gewissen Ausnahmen) der Punkt C näher an R liegen, als der Punkt B, oder es muss die Linie RC kürzer sein, als die Linie RB.

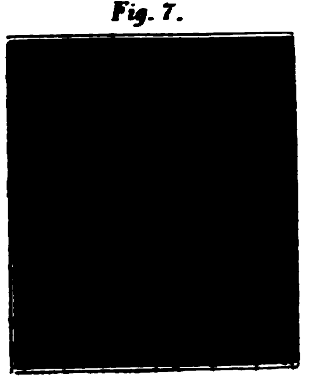
Hiernach wird das Verfahren sowol, wie die geometrische Bedeutung einer Kettenbruchsentwickelung und der Näherungsbrüche klar geworden sein. Es kommt nun darauf an, die ununterbrochene Verkürzung der Linien RA, RB, $RC \ldots$, d. i. die ununterbrochene Verkleinerung des numerischen Werthes der Differenzen $K - K_0$, $K - K_1$, $K - K_2 \ldots$ nachzuweisen und die etwaigen Ausnahmen zu charakterisiren.

Zu diesem Ende stellen wir erst noch einige charakteristische

Eigenthümlichkeiten der Kettenbruchsentwickelungen nach dem Prinzipe der absolut kleinsten Reste heraus.

III. **Es sei in Figur 7 *AB* irgend eine gerade Linie und *Oed* ein durch den Nullpunkt gehender Kreis, dessen Mittelpunkt *C* in dem von *O* auf *AB*** gefällten Perpendikel *OD* liegt und dessen Durchmesser *Od* der absoluten Länge nach die Reziproke des Perpendikels *OD* ist; man habe also, wenn $OD = D$ und $Od = d$ gesetzt wird, $d = \frac{1}{D}$ oder $D = \frac{1}{d}$. Alsdann **besteht zwischen jener Geraden und diesem Kreise folgende bemerkenswerthe Beziehung.**

Fig. 7.



Wenn man vom Nullpunkte *O* aus irgend eine gerade Linie *OF* zieht, welche die Gerade in *E* und den Kreis in *e* schneidet, und man setzt $OE = E$ und $Oe = e$; so ist stets $e = \frac{1}{E}$ oder $E = \frac{1}{e}$. Denn zieht man die Linie *de*; so ist in den beiden ähnlichen Dreiecken *Ode* und *OED*

$$e : d = D : E, \quad \text{also} \quad e = \frac{dD}{E} = \frac{1}{E}$$

Hieraus folgt nun, dass wenn *F* ein in der Richtung *OE* jenseit der Geraden *AB* liegender Punkt, also $OF = F > E$ ist, $\frac{1}{F} < \frac{1}{E}$ d. i. $< e$ sein wird, dass also der Endpunkt *e* jeder Länge, wie *OF*, welche jenseit der Geraden endigt, innerhalb des Kreises liegt. Ebenso folgt, dass der Endpunkt *g* der Reziproke jeder Länge, wie *OG*, welche diesseit der Geraden endigt, ausserhalb des Kreises liegt, wobei natürlich die umgekehrten Längen *Oe*, *Of*, *Og* immer in derselben Richtung der korrespondirenden Längen *OE*, *OF*, *OG* zu nehmen sind.

Diese Eigenschaft, wonach die Gerade und der Kreis die entsprechenden Gränzen resp. für die vom Nullpunkte aus gezogenen Linien und deren umgekehrte oder reziproke Längenwerthe bilden, erleidet keine Ausnahme, weder durch die besondere Richtung der Geraden, noch auch durch den Umstand, ob sich die Gerade und der Kreis schneiden oder nicht, d. h. ob $OD = D > 1$ oder < 1 sei. Für $D = 1$ berühren sich Beide in *D*. Ausserdem erhellet, dass die Beziehung zwischen der Geraden und dem Kreise dergestalt wechselseitig ist, dass man

leicht, wenn die Gerade gegeben ist, den zugehörigen Kreis, und wenn der Kreis gegeben ist, die zugehörige Gerade lediglich durch die Bedingung $d = \frac{1}{D}$ oder $D = \frac{1}{d}$ oder $d.D = 1$ bestimmen kann.

Des kürzeren Ausdrucks wegen wollen wir zwei Figuren wie ABC und abc in Figur 8, deren sämmtliche Vektoren in dem fraglichen umgekehrten Verhältnisse zueinander stehen, reziproke Figuren nennen. Diese Figuren können Flächenräume, Linienstücke oder auch einzelne Punkte sein.

Fig. 8.



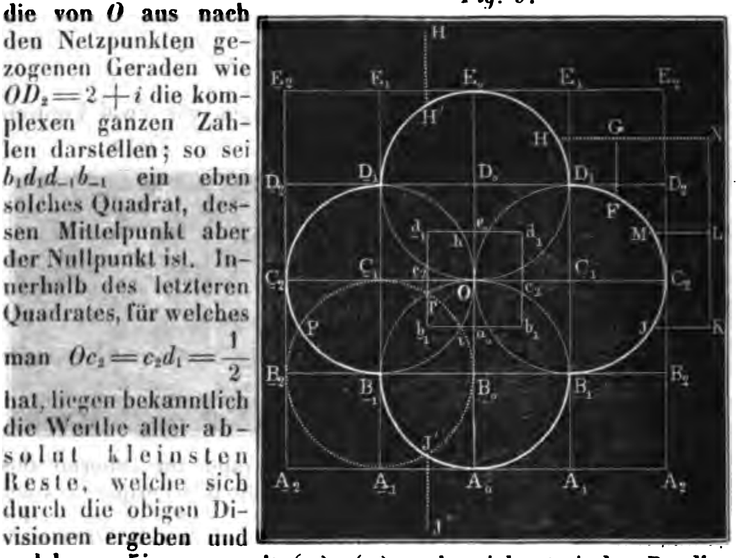
Allgemein ist die reziproke Figur eines Kreises wie ef wiederum ein Kreis EF. Die Zentrallinie Dd, sowie die gemeinschaftlichen äusseren Tangenten gehen durch den Nullpunkt O. Obgleich jedem Punkte in der Peripherie oder im Inneren des Einen Kreises ein reziproker Punkt resp. in der Peripherie oder im Inneren des anderen Kreises entspricht, indem z. B. $Oe = \frac{1}{OE}$, $Of = \frac{1}{OF}$ ist; so muss doch ausdrücklich darauf aufmerksam gemacht werden, dass die Mittelpunkte beider Kreise keine reziproke Lage haben.

Der Beweis des letzteren allgemeineren Satzes ist ähnlich zu führen, wie in dem vorhergehenden spezielleren Falle, wo der Eine Kreis durch den Nullpunkt ging, also $Oe = 0$ und $\frac{1}{Oe} = OE = \infty$ ist und demzufolge die vordere Seite des anderen Kreises bei F sich in einen Kreisbogen von unendlich grossem Radius, d. i. in eine gerade Linie verwandelte.

Wir bemerken noch, dass wenn für den Einen Kreis $Od = \sqrt{2}$, $de = 1$, also $Oe = \sqrt{2} - 1$ und $Of = \sqrt{2} + 1$ ist, für den reziproken Kreis $OE = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = Of$ und $OF = \frac{1}{\sqrt{2} + 1} = \sqrt{2} - 1 = Oe$ ist, dass also dann die beiden reziproken Kreise sich decken.

IV. Wenn in Fig. 9 die Seitenlänge OC_1 der netzförmigen Quadrate $=1$ ist, also die von O aus nach den Netzpunkten gezogenen Geraden wie $OD_2 = 2+i$ die komplexen ganzen Zahlen darstellen; so sei $b_1 d_1 d_{-1} b_{-1}$ ein eben solches Quadrat, dessen Mittelpunkt aber der Nullpunkt ist. Innerhalb des letzteren Quadrates, für welches man $Oc_2 = c_2 d_1 = \frac{1}{2}$ hat, liegen bekanntlich die Werthe aller a b s o l u t k l e i n s t e n R e s t e, welche sich durch die obigen Divisionen ergeben und welche vorhin resp. mit (s_0), (s_1) ... bezeichnet sind. Da diese Reste behuf der Bestimmung der Quotienten (r_1), (r_2) ... umzukehren sind; so ist es wichtig, die r e z i p r o k e Figur des Quadrates $b_1 d_1 d_{-1} b_{-1}$ zu kennen. Beschreibt man zu diesem Ende um die vier Punkte C_1, D_0, C_{-1}, B_0 Kreise, deren Radius $=1$, deren Durchmesser also $= 2 = \frac{1}{\frac{1}{2}}$ ist; so leuchtet ein, dass der ausserhalb aller jener Kreise liegende Flächenraum, welcher nach dem Nullpunkte hinzu durch die Bögen $C_2 D_1 E_0 D_{-1} C_{-2} B_{-1} A_0 B_1 C_2$ begränzt ist und sich jenseit dieser Gränze ins Unendliche erstreckt, dem fraglichen Quadrate reziprok ist.

Fig. 9.



Hieraus folgt, dass kein Quotient einer Kettenbruchsentwickelung mit absolut kleinsten Resten i n n e r h a l b der eben bezeichneten Figur $C_2 E_0 C_{-2} A_0$ liegen, also weder $=0$, noch $=\pm 1$, noch $=\pm i$ sein kann. Die kleinstmöglichen Quotienten einer solchen Entwickelung, vom zweiten (r_1) an, sind also $\pm 1 \pm i$, alsdann ± 2, $\pm 2i$ und hierauf $\pm 1 \pm 2i$, $\pm 2 \pm i$, welche resp. die absoluten Werthe $\sqrt{2}$, 2, $\sqrt{5}$ haben.

Dasselbe Resultat ist schon in §. 197, II. gefunden. Wir werden dasselbe jetzt aber noch durch einige interessante Beziehungen erweitern. Wenn nämlich ein Quotient von der Form $\pm 1 \pm i$, z. B. der Quotient $(r_1) = 1 + i = (OD_1)$, eingetreten

ist; so ist die **Richtung** des absolut kleinsten Restes (s_1) nicht mehr unbeschränkt; es kann vielmehr dieser Rest nur in dem Theile D_1FGHD_1 des um D_1 als Mittelpunkt beschriebenen Quadrates $\square_1$ liegen. Hätte sich dagegen $(r_1)=2=(OC_2)$ ergeben; so könnte der Rest nur in dem Theile $IKLM$ des um C_2 beschriebenen Quadrates liegen.

Denken wir uns nun zuerst die Figur D_1FGHD_1 parallel zu sich selbst mit D_1 an den Nullpunkt geschoben; so ergibt sich die Figur Ofd_1hO. Nehmen wir hiervon die Reziproke; so verwandeln sich die Geraden d_1h und d_1f in die Kreise D_1H' und D_1F, dagegen verwandeln sich die Kreise Oh und Of in die Geraden $H'H''$ und IK, welche sich ins Unendliche erstrecken. Die gesuchte reziproke Figur, welche einen in der unteren Ecke durch $KID_1H'H''$ begränzten Quadranten darstellt, enthält nur solche **ganze** Zahlen von der Form $a+bi$, in welchen sowol a, wie b **positiv** sind. Auf den Gränzlinien IK und $H'H''$ kann man jedoch auch, wenn man will, die ganzen Zahlen aus der Reihe B_1B_2 und $D_{-1}E_{-1}$ nehmen, wodurch also auch ganze Zahlen von den beiden Formen $a-i$ und $-1+bi$ möglich werden.

Beachtet man, dass bei der Quotientenbildung noch der Neigungswinkel der eben bestimmten Grösse mit entgegengesetzten Zeichen zu nehmen ist, wodurch in der Form $a+bi$ die Grösse b das Zeichen wechselt; so folgt, dass der auf den Quotienten $1+i$ zunächst folgende Quotient nothwendig von der Form $a-bi$, oder in besonderen Fällen, wenn man will, von der Form $a+i$ oder $-1-bi$ sein muss, worin a und b positiv gedacht sind. Überhaupt erkennt man, dass der Quotient, welcher auf

$1+i$ folgt, nur die Form $a-bi$, zuweilen auch,
wenn man will, $a+i$ und $-1-bi$
$1-i$ » » » » $a+bi$, zuweilen auch,
wenn man will, $a-i$ » $-1+bi$
$-1+i$ » » » » $-a-bi$, zuweilen auch,
wenn man will, $-a+i$ » $1-bi$
$-1-i$ » » » » $-a+bi$, zuweilen auch,
wenn man will, $-a-i$ » $1+bi$

besitzen kann, insofern der erstere Quotient nicht derjenige vom Zeiger 0 ist.

Wäre der Quotient $(r_1)=2$ gewesen, so trage man die Figur C_2FKLMC_2 mit C_2 an den Nullpunkt und suche die reziproke Figur. Die letztere wird die in der Nähe des Nullpunktes durch $I''I'C_2H'H''$ begränzte halbe Koordinatenebene sein. Hieraus ergibt sich, dass auf den Quotienten

2 nur ein anderer von der Form $a \pm bi$,
zuweilen auch, wenn man will, $-1 \pm bi$
-2 nur ein anderer von der Form $-a \pm bi$,
zuweilen auch, wenn man will, $1 \pm bi$
$2i$ nur ein anderer von der Form $\pm a - bi$,
zuweilen auch, wenn man will, $\pm a + i$
$-2i$ nur ein anderer von der Form $\pm a + bi$,
zuweilen auch, wenn man will, $\pm a - i$

folgen kann, insofern der erstere Quotient nicht derjenige vom Zeiger 0 ist.

Wäre endlich der Quotient $(r_1) = 2 + i$ gewesen; so hat man die Figur *NGFMLN* so an den Nullpunkt zu tragen, dass D_2 in O fällt. Dies gibt $d_1 d_{-1} p i b_1 d_1$. Die reziproken Linien der Seiten $d_1 d_{-1}$, $d_{-1} p$, $i b_1$, $b_1 d_1$ sind die Kreisbögen $D_1 D_{-1}$, $D_{-1} P$, $I' B_1$, $B_1 D_1$. Was die Reziproke der krummen Seite pi betrifft; so ist dieselbe ein Bogen des um B_{-1} mit der Längeneinheit beschriebenen Kreises, für welchen ausserdem $OB_{-1} = \sqrt{2}$ ist. Der reziproke Kreis ist also nach III., mit diesem identisch; die reziproken Punkte Beider liegen aber auf entgegengesetzten Seiten des Mittelpunktes B_{-1}. Demnach ist der Bogen $PB_{-2}A_{-1}I'$ reziprok dem Bogen pi. Hierdurch fällt der Endpunkt B_{-1} der ganzen Zahl $-1-i$ aus dem Bereiche derjenigen ganzen Zahlen, welche den in der fraglichen Figur liegenden Grössen reziprok sein können. Auf diesem Wege erhellet, dass auf den Quotienten

$2+i$	und	$1+2i$	nicht der Quotient	$-1+i$
$2-i$	»	$1-2i$	» » »	$-1-i$
$-2+i$	»	$-1+2i$	» » »	$1+i$
$-2-i$	»	$-1-2i$	» » »	$1-i$

wol aber jeder andere, welcher absolut $\geqq \sqrt{2}$ ist, folgen kann, insofern der erstere Quotient nicht derjenige vom Zeiger 0 ist.

Endlich sieht man leicht ein, dass bei keinen anderen, als als den vorstehend bezeichneten Quotienten der Spielraum für den nächstfolgenden Quotienten anders, als durch die allgemeine Bedingung beschränkt ist, dass der Letztere $\geqq \sqrt{2}$ sein müsse.

V. Aus den vorstehenden Beziehungen ergibt sich das Gesetz über die Annäherung der Näherungsbrüche folgendermaassen.

Die Nenner der Näherungsbrüche sind von dem ersten Quotienten (r_0), welcher unter Umständen den absoluten Werth 0, 1 und $\sqrt{2}$ haben kann, ganz unabhängig. Der erste Nenner N_0 ist stets $=1$, also grösser als der vorhergehende Nenner N_{-1}, welcher stets $=0$ ist. Angenommen, von Quotienten (r_1)

an habe man erst eine beliebige Anzahl von Quotienten, welche absolut sämmtlich $> \sqrt{2}$ sind. Alsdann muss nach §. 197, III. jeder spätere Nenner numerisch entweder $>$ oder $=$ dem vorhergehenden sein. Auf diese Quotienten folge nunmehr Einer, welcher absolut $= \sqrt{2}$ sei; alsdann muss der weiter folgende $> \sqrt{2}$ sein und zugleich der im Vorstehenden angegebenen Bedingung hinsichtlich seiner Richtung genügen. Nehmen wir daher, um die Vorstellung zu fixiren, von der gedachten Stelle folgende Reihenfolge der Quotienten und Nenner an, worin $r, r_1 \ldots$ sowie $N, N_1 \ldots$ positive Zahlen bezeichnen.

n	(r)	(N)
n		$(N) = Ne^{\alpha i}$
$n+1$		$(N_1) = N_1 e^{\alpha_1 i}$
$n+2$	$(r_2) = r_2 e^{\varphi_2 i}$	$(N_2) = N_2 e^{\alpha_2 i}$
$n+3$	$(r_3) = r_3 e^{\varphi_3 i}$	$(N_3) = N_3 e^{\alpha_3 i}$

Hierin sei der Quotient $(r_2) = 1 + i$, also $r_2 e^{\varphi_2 i} = \sqrt{2} e^{\frac{\pi}{4} i}$; alsdann muss $r_3 > \sqrt{2}$ und (r_3) von der Form $a - bi$ sein, mithin der Winkel φ_3 zwischen 0 und $-\frac{\pi}{2}$ liegen. Ferner sei unter den Nennern $N_1 \geqq N$. Jetzt hat man für den Nenner (N_2)

$$(9) \qquad (N_2) = (r_2)(N_1) + (N)$$

$$= \sqrt{2} N_1 e^{\left(\frac{\pi}{4} + \alpha_1\right) i} + Ne^{\alpha i}$$

und für den Nenner (N_3)

$$(10) \qquad (N_3) = (r_3)(N_2) + (N_1)$$

$$= \sqrt{2}\, r_3 N_1 e^{\left(\frac{\pi}{4} + \alpha_1 + \varphi_3\right) i} + r_3 N e^{(\alpha + \varphi_3) i} + N_1 e^{\alpha_1 i}$$

Der numerische Werth von (N_2) wird nun nicht immer $>$ oder $=$ dem von (N_1) sein. Wol aber ist stets der von $(N_3) >$ als der von (N_1). Um Dies zu erkennen, schreiben wir nach Gl. (10)

$$(N_3) = \sqrt{2} r_3 N_1 \cos\left(\frac{\pi}{4} + \alpha_1 + \varphi_3\right) + r_3 N \cos(\alpha + \varphi_3) + N_1 \cos \alpha_1$$
$$+ [\sqrt{2} r_3 N_1 \sin\left(\frac{\pi}{4} + \alpha_1 + \varphi_3\right) + r_3 N \sin(\alpha + \varphi_3) + N_1 \sin \alpha_1] i$$

Nehmen wir die Summe der Quadrate der absoluten Werthe des reellen und imaginären Theiles von (N_3); so kommt

$$N_3^2 = 2 r_3^2 N_1^2 + r_3^2 N^2 + N_1^2 + 2\sqrt{2} r_3^2 N N_1 \cos\left(\frac{\pi}{4} + \alpha_1 - \alpha\right)$$
$$+ 2\sqrt{2} r_3 N_1^2 \cos\left(\frac{\pi}{4} + \varphi_3\right) + 2 r_3 N N_1 \cos(\alpha - \alpha_1 + \varphi_3)$$

Um das Minimum dieses Werthes zu bestimmen, beachte man, dass $\cos\left(\frac{\pi}{4}+\alpha_1-\alpha\right)$ und $\cos(\alpha-\alpha_1+\varphi_3)$ tiefstens auf -1 herabsinken können. Da aber φ_3 zwischen 0 und $-\frac{\pi}{2}$ liegt; so ergibt sich der kleinste Werth von $\cos\left(\frac{\pi}{4}+\varphi_3\right)$ für $\varphi_3=-\frac{\pi}{2}$ und ist demnach $=\cos\left(-\frac{\pi}{4}\right)=\frac{1}{\sqrt{2}}$. Hiernach ist also unbedingt

$$N_3^2 \geqq 2r_3^2N_1^2+r_3^2N^2+N_1^2+2r_3N_1^2-2\sqrt{2}\,r_3^2NN_1-2r_3NN_1$$

und da $N_1\geqq N$ ist, auch

$$(11)\qquad N_3^2\geqq 2r_3^2N_1^2+r_3^2N^2+N_1^2-2\sqrt{2}\,r_3^2NN_1$$

Dass der Ausdruck auf der rechten Seite aber grösser als die Norm N_1^2 des Nenners (N_1) ist, oder dass man

$$2r_3^2N_1^2+r_3^2N^2+N_1^2-2\sqrt{2}\,r_3^2NN_1>N_1^2$$

$$\text{oder}\quad 2r_3^2N_1^2+r_3^2N^2-2\sqrt{2}\,r_3^2NN_1>0,\quad \text{d. i.}$$

$$r_3^2(\sqrt{2}\,N_1-N)^2>0\quad\text{oder}$$

$$r_3(\sqrt{2}\,N_1-N)>0$$

hat, leuchtet ein, weil schon $N_1\geqq N$ ist. Demnach hat man $N_3>N_1$, was zu beweisen war.

Ist nun $N_2<N_1$; so hat man wegen $N_3>N_1$ auch $N_3>N_2$. In diesem Falle kann also nach §. 196, Gl. (16) die Näherung bei dem Näherungsbruche K_2 gestört werden, indem man hierfür den Ausdruck

$$\frac{K-K_2}{K-K_1}=-\frac{(x_2)(N_1)}{(N_2)}$$

hat, welcher numerich >1 sein kann, sodass möglicherweise K_2 sich weiter von K entfernen kann, als K_1. Dagegen beginnt die Näherung sofort wieder beim Näherungsbruche K_3, und zwar liegt dieser Bruch nicht allein näher als K_2, sondern auch näher als K_1 an K. Das Erstere erhellet, weil $N_3>N_2$ ist. Das Letztere erhellet, weil aus der vorstehenden und aus der Gleichung

$$\frac{K-K_3}{K-K_2}=-\frac{(x_3)(N_2)}{(N_3)}$$

die dritte

$$\frac{K-K_3}{K-K_1}=\frac{(x_2)(x_3)(N_1)}{(N_3)}$$

folgt, worin $N_3 > N_1$, (x_2) und (x_3) numerisch $\leqq \frac{1}{\sqrt{2}}$, also $(x_2)(x_3)$ numerisch $\leqq \frac{1}{2}$ ist.

Wäre dagegen $N_2 \geqq N_1$; so folgt schon aus §. 197, dass, weil der Quotient (r_2) numerisch $> \sqrt{2}$ ist, $N_3 \geqq N_2$ sein wird. In diesem Falle wird also auch nicht einmal bei K_2 das Näherungsgesetz gestört.

Was die Zähler (M) der Näherungsbrüche betrifft; so folgen dieselben hinsichtlich ihres Wachsthumes einem gleichen Gesetze, wie die Nenner, obgleich von ihnen das Näherungsgesetz für die Näherungsbrüche gar nicht abhängt. Die Zähler werden jedoch vom ersten Quotienten (r_0) affizirt, welcher numerisch $= 0$, 1 und $\sqrt{2}$ sein kann.

Ist $r_0 = 0$; so ist $M_0 = 0$ und $M_1 = 1$, und man kann in diesem Falle die Betrachtung mit den beiden Zählern (M_0) und (M_1) beginnen.

Ist $r_0 = 1$; so ist $M_{-1} = 1$ und $M_0 = 1$, und man kann von den beiden Zählern (M_{-1}) und (M_0) ausgehen. Dasselbe kann geschehen, wenn $r_0 = \sqrt{2}$, also $M_{-1} = 1$ und $M_0 = \sqrt{2}$ ist.

VI. Das Gesetz der Näherungsbrüche lässt sich noch auf folgende Weise sehr klar geometrisch veranschaulichen.

In Figur 10 stellt die aus vier Halbkreisen bestehende Linie die Reziproke des um den Nullpunkt mit der Längeneinheit als Seite beschriebenen Quadrates dar. Das verzeichnete Netz der Quadrate ist durch die Punkte gelegt, welche in den Richtungen der Grundaxen resp. um $\frac{1}{2}$, $1\frac{1}{2}$, $2\frac{1}{2}$... vom Nullpunkte abstehen. Die Endpunkte der ganzen Zahlen liegen also in den Mittelpunkten der Quadrate dieses Netzes.

Fig. 10.



Die absolut kleinsten Reste (s), welche durch die Absonderung der zunächst liegenden ganzen Quotienten (r) entstehen,

sind Linien $\leqq \sqrt{2}$, welche von den eben genannten Mittelpunkten auslaufen und über die Gränze des betreffenden Quadrates nicht hinausreichen. Von diesen Quadraten sind die am Umfange der krummlinigen Figur liegenden unvollständig, und die einem solchen unvollständigen Quadrate angehörigen Reste können niemals über den krummlinigen Theil der Gränzlinie hinaustreten. Demnach wird unbedingt jeder Rest, wenn man ihn parallel zu sich selbst an den Nullpunkt trägt, innerhalb des mittleren Quadrates liegen, weil dasselbe vollständig ist.

Umgekehrt kann dagegen eine im mittleren Quadrate liegende, vom Nullpunkte auslaufende Linie unbedingt nur in jedes der vollständigen Quadrate von dessen Mittelpunkte aus parallel übertragen werden. Wäre das letztere Quadrat Eines der 16 unvollständigen Quadrate; so wäre es denkbar, dass bei der parallelen Übertragung die krumme Gränzlinie dieses Quadrates überschritten würde. Ein solcher Fall kann aber dann nicht eintreten, wenn die aus dem mittleren Quadrate in das unvollständige Quadrat zu übertragende Linie das Reziprokum einer Zahl ist, deren Endpunkt in demjenigen Theile der Koordinatenebene liegt, welcher nach den Betrachtungen sub IV. der mögliche Ort für die reziproken Werthe der aus dem unvollständigen Quadrate herrührenden Reste ist. Ein solches Verhältniss findet bei den nachfolgenden Untersuchungen stets statt, und demnach wird bei den vorkommenden Übertragungen niemals die Gränze der betreffenden Figur überschritten werden.

Jetzt sei $(OA) = (r_0)$, $(OA_1) = (r_1)$, $(OA_2) = (r_2)$ etc. resp. der 1ste, 2te, 3te etc. Quotient eines nach dem Prinzipe der numerisch kleinsten Reste entwickelten Kettenbruchs K.

Der erste Näherungsbruch ist $K_0 = (r_0)$ und die lineare Gränze für die Differenz $K - K_0$ bildet das um A beschriebene Quadrat $\square_0$, dessen Seite die Längeneinheit ist.

Um den zweiten Näherungsbruch $(K_1) = (r_0) + \frac{1}{(r_1)}$ zu bilden, nimmt man die Reziproke von $(OA_1) = (r_1)$ und überträgt dieselbe von dem inneren Quadrate in das Quadrat $\square_0$ vom Punkte A aus. Nun ist aber die Reziproke des ganzen (hier unvollständigen) Quadrates $\square_1$, dessen Mittelpunkt A_1 ist, nur ein Theil des mittleren Quadrates, welcher durch den Abschnitt in der oberen Ecke links versinnlicht ist. Überträgt man diesen Abschnitt in das Quadrat $\square_0$ bei A; so bildet derselbe die Gränze für die Differenz $K - K_1$. Man sieht, dass diese Gränze ganz innerhalb der quadratischen Gränze für $K - K_0$ liegt, also enger ist.

Um den dritten Näherungsbruch $K_2 = (r_0) + \frac{1}{(r_1) + \frac{1}{(r_2)}}$ zu bilden, nimmt man die Reziproke von $(OA_2) = (r_2)$. Der Endpunkt desselben liegt offenbar in dem Reziproken des ganzen Quadrates $\square_2$, welches um A_2 beschrieben ist. Dasselbe macht einen anderen Theil des mittleren Quadrates aus, und ist darin durch eine kleine, von dem Abschnitte in der Ecke getrennte Kreisfläche dargestellt. Überträgt man diese kleine Kreisfläche in das Quadrat $\square_1$ bei A_1; so muss sie ganz in dessen Innern liegen, wie aus dem Früheren unzweideutig erhellet. Demnach liegt auch die Übertragung von $\frac{1}{(r_2)}$ in das Quadrat $\square_1$ oder der Endpunkt von $(r_1) + \frac{1}{(r_2)}$ ganz in dessen Innern. Nimmt man jetzt das Reziproke von $(r_1) + \frac{1}{(r_2)}$; so fällt dasselbe ganz in den Abschnitt an der oberen Ecke hinein, und zwar liegt dasselbe in derjenigen Figur, welche die Reziproke des im Quadrate $\square_1$ verzeichneten Kreises bildet. Die letztere Figur ist durch den noch kleineren Kreis, welcher innerhalb des Abschnittes an der Ecke verzeichnet ist, dargestellt und bildet die Gränze für $\frac{1}{(r_1) + \frac{1}{(r_2)}}$. Überträgt man endlich diesen Werth in das Quadrat $\square_0$ bei A; so liegt sein Endpunkt oder der Endpunkt von $K_2 = (r_0) + \frac{1}{(r_1) + \frac{1}{(r_2)}}$ ganz im Innern der dorthin übertragenen, von dem Abschnitte an der Ecke ganz umschlossenen Figur. Die Gränzlinie für die Differenz $K - K_2$ hat sich also noch weiter verengt.

Hieraus wird das Näherungsgesetz deutlich geworden sein. Wir bemerken noch, dass dieses Gesetz bei einem Kettenbruche, welcher nicht nach dem Prinzipe der numerisch kleinsten Reste gebildet ist, deshalb nicht nachweisbar ist, weil alsdann die in unvollständige Quadrate übertragenen Linien nicht mit Nothwendigkeit ganz in das Innere dieser Quadrate, auch die fraglichen Gränzfiguren nicht nothwendig ineinander zu fallen brauchen.

VII. Aus allem Vorstehenden erhellet, dass wenn man eine Reihenfolge von Quotienten annimmt, welche den entwickelten Bedingungen nicht widersprechen, dieselben immer

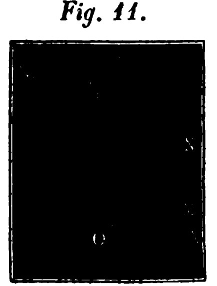
eine Kettenbruchsentwickelung mit numerisch kleinsten Resten darstellen; im Gegentheile aber nicht.

Demnach ist auch jeder Näherungsbruch K_n durch die Quotientenfolge (r_0), $(r_1) \dots (r_n)$, aus denen er besteht, in einen Kettenbruch mit absolut kleinsten Resten entwickelt.

VIII. Endlich machen wir darauf aufmerksam, indem wir irgend einen Näherungsbruch in der Form

$$K_n = \frac{(M)}{(N)} = \frac{Me^{\mu i}}{Ne^{\nu i}} = \frac{M}{N} e^{(\mu - \nu)i}$$

schreiben, dass weil nach dem obigen Näherungsgesetze die Grösse K_n nicht bloss nach ihrem absoluten Werthe, sondern auch nach ihrer Richtung der Grösse K immer näher und näher kommt, je höher man den Zeiger n nimmt, nothwendig nicht bloss der absolute Werth $\frac{M}{N}$, sondern auch die Winkelgrösse $\mu - \nu$ einem konstanten Werthe entgegenstrebt.


Fig. 11.

Wenn also in Figur 11 (OM) und (ON) nach Länge und Richtung den Zähler und Nenner irgend eines Näherungsbruches K_n darstellt; so nähert sich nicht bloss das Verhältniss zwischen den beiden absoluten Längen von OM und ON, sondern auch der zwischen diesen beiden Linien liegende Winkel $MON = \mu - \nu$ einem bestimmten Werthe, d. h. das über Zähler und Nenner der sukzessiven Näherungsbrüche entworfene Dreieck, wie MON, M_1ON_1 u.s.w., wird immer mehr einem bestimmten Dreiecke ähnlich.

Man kann also mit Hülfe der Kettenbrüche die Aufgabe lösen, ein gegebenes Dreieck M_1ON_1, für welches

$$K = \frac{A + Bi}{A_1 + B_1 i} = \frac{(M_1)}{(N_1)}$$

ist, möglichst genau durch Dreiecke wie MON darzustellen, für welche die rechtwinkligen Koordinaten der Punkte M und N möglichst kleine ganze Zahlen sind.

§. 199. *Auflösung der unbestimmten Gleichungen vom ersten Grade in komplexen Zahlen.*

I. Wir suchen jetzt die Auflösungen der Gleichung

(1) $$Ax - By = C$$

in der Voraussetzung, dass die Koeffizienten A, B, C beliebige reelle, imaginäre oder komplexe ganze Zahlen seien, indem wir

für x und y alle zulässigen reellen, imaginären und komplexen ganzen Zahlen ermitteln.

Man kann zu diesem Ende offenbar die Methode des §. 28, welche eine sukzessive Aussonderung der Ganzen bezweckt, in Anwendung bringen, wenn man die zu beschaffenden Divisionen stets mit numerisch kleinsten Resten ausführt.

Man kann aber auch nach §. 30 und 32 die Kettenbrüche zu Hülfe nehmen, indem man erst eine Auflösung der Gleichung

(2) $$Ax' - By' = 1$$

sucht, und hierauf

(3) $$x = Cx' + Bw, \qquad y = Cy' + Aw$$

setzt.

Gleichviel, nach welcher Methode man verfährt, und auch dann, wenn A, B, C reelle Zahlen sind, immer hat man behuf Erzielung der grössten Allgemeinheit unter der Willkürlichen w irgend eine komplexe ganze Zahl zu verstehen.

Die Auflösung ist auch hier unmöglich, wenn A und B ein gemeinschaftliches Maass besitzen, welches nicht in C enthalten ist. Man kann daher bei einer möglichen Gleichung stets dafür sorgen, dass A und B vollkommen relativ prim werden.

Es wird hier, wie in §. 30, bemerkt, dass wenn man die Kettenbrüche anwendet, also den Werth von $\frac{A}{B}$ in einen Kettenbruch $\frac{M_n}{N_n}$ entwickelt, danach gesehen werden muss, dass bei der Reduktion dieses Kettenbruches die beiden Grössen M_n und N_n nicht bloss nach ihrem absoluten Werthe, sondern auch nach ihrem Zeichen resp. gleich A und B werden. Das Letztere kann, wenn es sich nicht von selbst einstellt, nach §. 196, III. stets leicht erreicht werden, indem man für M_{-1} und N_{-2} die richtige Potenz von i setzt oder die Zähler und Nenner aller Näherungsbrüche mit dieser Potenz multiplizirt. Erhalten hierdurch die Grössen M_{-1} und N_{-2} den Werth ± 1; so gilt die Gl. (13) in §. 197 und man hat als Auflösung der vorstehenden Gl. (2)

(4) $$x' = (-1)^{n-1} N_{n-1}, \qquad y' = (-1)^{n-1} M_{n-1}$$

Erhalten dagegen die Grössen M_{-1} und N_{-2} den Werth $\pm i$; so gilt die Gl. (14) in §. 197 und man hat

(5) $$x' = (-1)^n N_{n-1}, \qquad y' = (-1)^n M_{n-1}$$

II. Beispiel 1. Es sei gegeben

$$(3 + 4i)x - (1 + 2i)y = 5$$

Hier ist, wenn man die Kettenbrüche in Anwendung bringt, $\frac{A}{B}=\frac{3+4i}{1+2i}=\frac{M_n}{N_n}$ zu entwickeln. Dies gibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	2	2	1
1	$1+2i$	$3+4i$	$1+2i$

Hier hat man nach den Beziehungen (4)

$$x'=(-1)^0 N_0=1, \qquad y'=(-1)^0 M_0=2$$

also

$$x=5\,.\,1+(1+2i)(v+wi)=5+v-2w+(2v+w)i$$
$$y=5\,.\,2+(3+4i)(v+wi)=10+3v-4w+(4v+3w)i$$

Hierin stellt $v+wi$ eine willkürliche ganze Zahl oder v und w zwei willkürliche reelle ganze Zahlen dar. So hat man z. B. für $v=1$, $w=1$

$$x=4+3i, \qquad y=9+7i$$

III. Beispiel 2. Es sei gegeben

$$(2+30i)x-(7+10i)y=3-2i$$

Hier ist bei Zuhülfenahme der Kettenbrüche $\frac{A}{B}=\frac{2+30i}{7+10i}=\frac{M_n}{N_n}$ zu entwickeln. Dies gibt

n	a_n	M_n	N_n
-2		0	1
-1		1	0
0	$2+i$	$2+i$	1
1	$1-3i$	$6-5i$	$1-3i$
2	$3+2i$	$30-2i$	$10-7i$

Damit hier auch dem Zeichen nach $M_n=A$ und $N_n=B$ werde, muss $M_{-1}=i$ und $N_{-2}=i$ genommen werden. Hierdurch wird

$$M_{n-1}=M_1=5+6i, \qquad N_{n-1}=N_1=3+i$$

und da jetzt die Beziehungen (5) gelten; so ist

$$x'=(-1)^2 N_1=3+i, \qquad y'=(-1)^2 M_1=5+6i$$

folglich

$$x=(3-2i)(3+i)+(7+10i)(v+wi)=11+7v-10w+(-3+10v+7w)i$$
$$y=(3-2i)(5+6i)+(2+30i)(v+wi)=27+2v-30w+(8+30v+2w)i$$

So hat man z. B. für $v=0$, $w=0$

$$x=11-3i, \qquad y=27+8i$$

IV. Wenn man die Koeffizienten A und B in Gl. (1)

$$(6) \qquad A=a_0+a_1 i, \qquad B=b_0+b_1 i$$

setzt; so erkennt man leicht, dass die allgemeine Auflösung der Gleichung (1) in der Form

$$(7) \qquad \begin{cases} x=p_0+b_0 v-b_1 w+(p_1+b_1 v+b_0 w)i \\ y=q_0+a_0 v-a_1 w+(q_1+a_1 v+a_0 w)i \end{cases}$$

enthalten ist.

Will man die hierdurch dargestellten reellen Werthe von x und y ermitteln; so hat man diejenigen ganzen Werthe von v und w aufzusuchen, für welche gleichzeitig

$$(8) \qquad \begin{cases} p_1 + b_1 v + b_0 w = 0 \\ q_1 + a_1 v + a_0 w = 0 \end{cases}$$

ist. Die beiden Grössen v und w sind also aus zwei Gleichungen vom ersten Grade zu bestimmen.

Wenn Eine der beiden Grössen v, w in der ersten und die andere in der zweiten der vorstehenden beiden Gleichungen (8) vorkommt (gleichviel, ob sonst jede dieser Gleichungen nur Eine der beiden Grössen v, w oder beide zugleich enthält); so kann die Auflösung der Gleichungen (8) nur einen einzigen Werth für v und auch nur einen einzigen für w ergeben. In diesem Falle, welcher stets eintritt, wenn die beiden Koeffizienten A und B der gegebenen Gl. (1) vollständig komplex sind, ist also nur eine einzige Auflösung der Gl. (1) in reellen Zahlen denkbar. Die Existenz einer solchen Auflösung setzt aber auch ferner noch voraus, dass die Werthe von v und w aus Gl. (8) ganze Zahlen seien.

So findet man für das erste der obigen Beispiele aus den Gleichungen

$$2v + w = 0$$
$$4v + 3w = 0$$

die beiden ganzen Werthe $v = 0$, $w = 0$. Die betreffende Gleichung hat also die einzige reelle Auflösung $x = 5$, $y = 10$.

Dagegen können in dem zweiten der obigen Beispiele die beiden Gleichungen

$$-3 + 10v + 7w = 0$$
$$8 + 30v + 2w = 0$$

nur durch die gebrochenen Werthe $v = -\frac{31}{95}$, $w = \frac{17}{19}$ erfüllt werden. Die betreffende Gleichung hat also keine reelle Auflösung.

Wenn aber jede der beiden Gleichungen (8) nur Ein und dieselbe der beiden Grössen v, w enthält, oder auch dann, wenn in Einer jener Gleichungen gar keine dieser beiden Grössen vorkommt, kann es eine unendliche Menge reeller Auflösungen der Gl. (1) geben. Dieselben finden sich durch diejenigen ganzen Werthe von v und w, welche den Gleichungen (8) ein Genüge leisten.

V. Was die Auflösung der unbestimmten Gleichungen vom ersten Grade mit mehr als zwei Unbekannten in komplexen Zahlen anlangt; so ist dieselbe nach den in §. 34 ff. entwickelten Prinzipien unter Anwendung der vorstehenden allgemeineren Zahlengesetze zu bewirken, indem man schliesslich für alle Willkürlichen ganze komplexe Zahlformen einführt.

Zehnter Abschnitt.

Unendliche Kettenbrüche, unbestimmte Gleichungen vom zweiten Grade

und

Grundlehren der Kongruenz in komplexen Zahlen.

---

§. 200. *Entwickelung der komplexen Wurzel einer quadratischen Gleichung in einen Kettenbruch.*

I. Wir gehen jetzt darauf aus, den Ausdruck $K=\frac{\sqrt{D}+P_0}{Q_0}$, worin D, P_0, Q_0 beliebige komplexe, aber ganze Zahlen seien, in einen Kettenbruch zu entwickeln, indem wir hier, wie in §. 59 voraussetzen, dass $D-P_0^2$ durch Q_0 theilbar oder $\frac{D-P_0^2}{Q_0}$ eine ganze Zahl Q_{-1} sei, was man in allen Fällen leicht bewirken kann.

Es leuchtet ein, dass die Grundformeln der §§. 59 und 61, durch welche die Grössen P_n, Q_n, a_n voneinander abhängen, fortwährend Gültigkeit behalten, welche willkürliche Werthe man auch für die Quotienten a_n einführen möge. Wenn also aus dem Gliede $x_n=\frac{\sqrt{D}+P_n}{Q_n}$ entweder durch beliebige Wahl oder nach einer sonstigen Bedingung der Quotient a_n bestimmt ist; so kann man behuf Berechnung der Grössen P_{n+1} und Q_{n+1} für das nächstfolgende Glied x_{n+1} immer die Formeln

(1) $$P_{n+1}=a_nQ_n-P_n$$

(2) $$Q_{n+1}=\frac{D-P^2_{n+1}}{Q_n}$$

in Anwendung bringen. Q_{n+1} wird stets eine ganze Zahl werden, und man führt die zur Ermittelung dieser Grösse dienende Division aus, indem man, wenn $Q_n = q + q'i$ ist, nach der Formel

$$(3) \qquad Q_{n+1} = \frac{(D - P^2_{n+1})(q - q'i)}{q^2 + q'^2}$$

verfährt.

II. Damit nun aber der sich ergebende Kettenbruch konvergire, dergestalt, dass die höheren Näherungsbrüche immer genauer den Werth von K darstellen, hat man das Prinzip der absolut kleinsten Reste in Anwendung zu bringen, also für den Quotienten a_n diejenige ganze Zahl zu nehmen, welche der Grösse $\frac{\sqrt{D} + P_n}{Q_n}$ am nächsten kommt, oder für welche der absolute Werth des Restes $\leqq \frac{1}{\sqrt{2}}$ ist. Um diesen Quotienten zu finden, kann man nach Einer der beiden nachstehenden Regeln verfahren.

III. Zuvörderst jedoch bemerken wir, dass sich ein Ausdruck von der allgemeinen Form $\sqrt{a + bi}$ nach einer bekannten Formel in einen anderen verwandelt, in welchem das Reelle vom Imaginären getrennt ist, indem man setzt

$$(4) \qquad \sqrt{c + di} = \sqrt{\frac{1}{2}(\sqrt{c^2 + d^2} + c)} \pm \sqrt{\frac{1}{2}(\sqrt{c^2 + d^2} - c)}\,.\,i$$

Hierin ist das erste Glied stets **positiv**, das zweite ist dagegen resp. **positiv oder negativ** zu nehmen, jenachdem die Grösse d **positiv oder negativ** ist.

IV. Nehmen wir jetzt an, es handele sich um die Bestimmung desjenigen in der Grösse

$$(5) \qquad K = \frac{\sqrt{D + D'i} + P + P'i}{Q + Q'i}$$

enthaltenen ganzen Quotienten $a + a'i$, welcher den absolut kleinsten Rest zurücklässt; so kann man, indem man Zähler und Nenner mit $Q - Q'i$ multiplizirt, zuvörderst schreiben

$$K = \frac{\sqrt{(D + D'i)(Q - Q'i)^2} + (P + P'i)(Q + Q'i)}{Q^2 + Q'^2}$$

ein Ausdruck, welcher nach gehöriger Berechnung die Form

$$(6) \qquad K = \frac{\sqrt{E + E'i} + R + R'i}{Q^2 + Q'^2}$$

annimmt.

Setzt man jetzt nach der Formel (4)

$$(7) \qquad \sqrt{E+E'i}=F+F'i$$

worin F und F' im Allgemeinen keine ganzen, sondern irrationale Zahlen darstellen; so erhält man

$$(8) \qquad K=\frac{F+R}{Q^2+Q'^2}+\frac{F'+R'}{Q^2+Q'^2}i$$

Jetzt ist für a diejenige ganze Zahl, welche dem Werthe $\frac{F+R}{Q^2+Q'^2}$ am nächsten kommt, und für a' diejenige anzunehmen, welche dem Werthe $\frac{F'+R'}{Q^2+Q'^2}$ am nächsten kommt.

Um auf die Berechnung der irrationalen Grössen F und F' nicht mehr Mühe zu verwenden, als nöthig ist, beachte man, dass es darauf ankommt, die Werthe von $\frac{F+R}{Q^2+Q'^2}$ und von $\frac{F'+R'}{Q^2+Q'^2}$ auf halbe Einheiten genau zu kennen, sodass man, wenn n eine ganze Zahl bezeichnet, mit Bestimmtheit die beiden Gränzen $n-\frac{1}{2}$ und $n+\frac{1}{2}$ erkennt, zwischen welchen jeder der fraglichen Werthe liegt. Dies wird erreicht, wenn man das Doppelte dieser Werthe auf ganze Einheiten genau anzugeben vermag, wobei man sich darauf beschränken kann, diejenige ganze Zahl zu ermitteln, deren absoluter Werth zunächst unterhalb des fraglichen Duplums liegt.

Demnach multiplizire man Zähler und Nenner der rechten Seite von Gl. (6) mit 2 und schreibe

$$(9) \qquad K=\frac{\sqrt{4(E+E'i)}+2(R+R'i)}{2(Q^2+Q'^2)}$$

und berechne die Grösse $\sqrt{4(E+E'i)}$ auf ganze Einheiten genau. Dies geschieht, indem man nach der Formel (4)

$$(10) \qquad \sqrt{4(E+E'i)}=\sqrt{2(\sqrt{E^2+E'^2}+E)}\pm\sqrt{2(\sqrt{E^2+E'^2}-E)}.i$$
$$=\sqrt{\sqrt{4(E^2+E'^2)}+2E}\pm\sqrt{\sqrt{4(E^2+E'^2)}-2E}.i$$

setzt. In dieser Formel braucht man den Werth von $\sqrt{4(E^2+E'^2)}$ ebenfalls nur auf ganze Einheiten genau zu nehmen. Ist dann m die zunächst unterhalb $\sqrt{4(E^2+E'^2)}$ liegende ganze Zahl; so braucht man auch $\sqrt{m+2E}$ und $\sqrt{m-2E}$ nur auf ganze Einheiten genau zu nehmen. Alsdann ergibt sich aus Gl. (9) mit Leichtigkeit der gesuchte Quotient $a+a'i$, indem man die Division mit $2(Q^2+Q'^2)$ in den reellen und in den

imaginären Theil des Zählers bis auf Eine Dezimalstelle ausführt, wodurch sich sofort die zunächst liegenden ganzen Zahlen a und a' kenntlich machen.

Obgleich man bei den vorhergehenden Berechnungen der ganzen Zahlen nicht in Dezimalstellen einzutreten braucht; so schützt man sich doch sicherer vor Irrthümern, wenn man hinter den ausgeworfenen ganzen Zahlen, welche numerisch kleiner sein sollen, als die betreffenden Grössen und sich vermöge ihres Zeichens bald durch Addition, bald durch Subtraktion miteinander verbinden, ein Dezimalkomma und einige Punkte setzt.

Wäre z. B.

$$K = \frac{\sqrt{4+5i}+1+i}{1+2i}$$

gegeben; so multiplizirt man sofort Zähler und Nenner mit $2(1-2i)$. Dies gibt

$$K = \frac{\sqrt{32-124i}+6-2i}{10}$$

Nun hat man nach der Formel (4), welche jetzt sogleich

$$(11) \qquad \sqrt{c+di} = \sqrt{\sqrt{\left(\frac{c}{2}\right)^2+\left(\frac{d}{2}\right)^2}+\frac{c}{2}} \pm \sqrt{\sqrt{\left(\frac{c}{2}\right)^2+\left(\frac{d}{2}\right)^2}-\frac{c}{2}}\,.\,i$$

geschrieben werden kann,

$$\begin{aligned}\sqrt{32-124i} &= \sqrt{\sqrt{16^2+62^2}+16} - \sqrt{\sqrt{16^2+62^2}-16}\,.\,i \\ &= \sqrt{\sqrt{4100}+16} - \sqrt{\sqrt{4100}-16}\,.\,i \\ &= \sqrt{64,\ldots+16} - \sqrt{64,\ldots-16}\,.\,i \\ &= \sqrt{80,\ldots} - \sqrt{48,\ldots}\,i \\ &= (8,\ldots) - (6,\ldots)i\end{aligned}$$

Demnach ist

$$K = \frac{(6+8,\ldots)-(2+6,\ldots)i}{10} = \frac{(14,\ldots)-(8,\ldots)i}{10}$$
$$= (1{,}4\ldots) - (0{,}8\ldots)i$$

und hieraus ergibt sich der Quotient

$$a + a'i = 1 - i$$

V. Das vorstehende Verfahren zur Berechnung der Quotienten $a+a'i$ wird durch die wiederholte Anwendung der Formel (4) und der vorhergehenden Umformungen etwas um-

ständlich. Folgendes Verfahren dürfte für die Praxis empfehlenswerther sein.

Man berechne Ein für alle Mal den in $\sqrt{D+D'i}$ enthaltenen reellen und imaginären Theil nach der Formel (4) bis auf eine gewisse Menge von Dezimalstellen, z. B. bis auf zwei. Dies gebe mit Vernachlässigung eines Fehlers, welcher höchstens $\frac{1}{100}$ der reellen oder der imaginären Einheit ausmachen kann,

$$(12) \qquad \sqrt{D+D'i} = \delta + \delta' i$$

Setzt man diesen Werth in den Ausdruck (5); so kommt

$$(13) \qquad K = \frac{P+\delta+(P'+\delta')i}{Q+Q'i}$$

und wenn man nun Zähler und Nenner mit $Q - Q'i$ multiplizirt,

$$(14) \qquad K = \frac{(P+\delta)Q-(P'+\delta')Q'}{Q^2+Q'^2} + \frac{(P+\delta)Q'+(P'+\delta')Q}{Q^2+Q'^2}$$

Wenn man diesen genäherten Werth für K nimmt; so kann der Fehler im Zähler des reellen oder imaginären Theiles höchstens das $Q \pm Q'$ fache, also der Fehler im reellen oder imaginären Theile selbst höchstens das $\left(\frac{Q \pm Q'}{Q^2+Q'^2}\right)$fache der letzten Dezimaleinheit von δ und δ' erreichen. Der absolute Werth des Bruches $\frac{Q \pm Q'}{Q^2+Q'^2}$ ist aber stets $\leqq 1$; demnach kann der fragliche Fehler höchstens Eine Einheit der letzten Dezimalstelle von δ und δ' betragen.

Hiernach kann man den Quotienten $a + a'i$ aus dem Näherungswerthe (14) bestimmen, indem man sowol im reellen, wie im imaginären Theile mit dem Nenner in den Zähler dividirt und die zunächst liegende ganze Zahl ermittelt. Diese Division ist in der Regel nur bis zur ersten Dezimalstelle auszuführen. Ergibt sich jedoch in dieser Stelle die Ziffer 4 oder 5, erhält man also, wenn n eine ganze Zahl darstellt, entweder n,4 oder n,5; so ist jene Division, um die Entscheidung herbeizuführen, fortzusetzen. Liefert diese Fortsetzung im ersten Falle die beiden Dezimalen 49 oder im zweiten Falle die beiden Dezimalen 50; so muss man noch fernere Dezimalen durch jene Division ermitteln. Überall aber darf man diese Division, wenn die Entscheidung nicht früher erfolgt, höchstens bis zur letzten Dezimalstelle von δ und δ' fortsetzen. Tritt nun bis zu dieser Dezimalstelle nicht die Entscheidung ein, ergibt sich also entweder der Werth n,49999... oder der Werth n,50000...; so kann durch die eingeschlagene Rechnung nicht mit Zuverlässig-

keit bestimmt werden, ob der gesuchte Quotient gleich n oder gleich $n+1$ sei. Man muss dann, wenn sich $n,49999\ldots$ ergeben hat, nachsehen, um wie viel der Zähler des betreffenden Theiles höchstens grösser werden kann, und wenn sich $n,50000\ldots$ ergeben hat, um wie viel jener Zähler höchstens kleiner werden kann, indem man bei δ und δ' die höchstmöglichen Fehler von Einer Einheit der letzten Dezimalstelle voraussetzt. Findet man durch Division in einen solchen Gränzwerth des Zählers als Gränzwerth für den Quotienten eine Zahl, welche im ersten Falle von unten her und im zweiten von oben her den entscheidenden Werth $n,5$ nicht erreicht; so hat man mit Zuverlässigkeit resp. n oder $n+1$ zu nehmen. Würde aber bei dieser Gränzrechnung der Werth $n,5$ resp. in der Richtung von unten nach oben oder von oben nach unten überschritten; so bleibt die Entscheidung zweifelhaft. Man muss dann entweder δ und δ' auf eine grössere Anzahl von Dezimalstellen berechnen, oder das vorhin sub IV. beschriebene Verfahren, welches niemals zu einem zweifelhaften Resultate führt, in Anwendung bringen.

Nachdem durch die vorstehende Rechnung ein Quotient gefunden ist, geht man mittelst der Formeln (1) und (2), in welchen nur genaue und niemals genäherte Grössen vorkommen, zu dem nächstfolgenden Gliede über. Man erkennt, dass für dieses, sowie für jedes spätere Glied behuf der Quotientenberechnung die bereits ermittelten Näherungswerthe δ und δ' immer wiederum verwendet werden können, also keine neue Ermittelung nöthig machen.

VI. Entwickeln wir nach dem letzteren Verfahren die Grösse $K=\frac{\sqrt{4+5i}+1+i}{1+2i}$, worin $D+D'i=4+5i$, $P_0+P_0'i=1+i$, $Q_0+Q_0'i=1+2i$ und der Vorbedingung gemäss $Q_{-1}+Q'_{-1}i=\frac{4+5i-(1+i)^2}{1+2i}=2-i$ eine ganze Zahl ist, in einen Kettenbruch, und nehmen wir nach Gl. (4) mit einer Annäherung auf Hundertstel

$$\sqrt{4+5i}=\sqrt{\frac{1}{2}(\sqrt{41}+4)}+\sqrt{\frac{1}{2}(\sqrt{41}-4)}\,.\,i$$
$$=2,28\ldots+1,09\ldots i$$

also $\delta+\delta'i=2,28+1,09i$. Hierdurch wird

$$K=x_0=\frac{3,28+2,09i}{1+2i}=\frac{7,46-4,47i}{5}=1,49-0,8i$$

Im reellen Theile dieses Werthes von x_0 ist aus den oben angeführten Gründen noch nicht mit Bestimmtheit zu erkennen,

ob sein Werth $<$ oder $> 1\frac{1}{2}$ sei. Da aber $Q = 1$, $Q' = 2$ ist; so kann der Zähler des reellen Theiles höchstens um $0{,}01 . 1 + 0{,}01 . 2 = 0{,}03$ grösser, also höchstens 7,49 werden. Da nun $\frac{7{,}49}{5} = 1{,}498$, also $< 1\frac{1}{2}$ ist; so hat man für den reellen Theil dieses Quotienten den Werth 1 zu nehmen. Es ist also

$$a_0 + a_0' i = 1 - i$$

Hieraus folgt nach Gl. (1) und (2)

$$P_1 + P_1' i = (1 - i)(1 + 2i) - (1 + i) = 2$$

$$Q_1 + Q_1' i = \frac{4 + 5i - 2^2}{1 + 2i} = 2 + i$$

$$x_1 = \frac{4{,}28 + 1{,}09i}{2 + i} = \frac{9{,}65 - 2{,}10i}{5} = 1{,}9 - 0{,}42i$$

also $a_1 + a_1 i = 2 - i$

$$P_2 + P_2' i = (2 - i)(2 + i) - 2 = 3$$

$$Q_2 + Q_2' i = \frac{4 + 5i - 3^2}{2 + i} = -1 + 3i$$

$$x_2 = \frac{5{,}28 + 1{,}09i}{-1 + 3i} = \frac{-2{,}01 - 16{,}93i}{10} = -0{,}2 - 1{,}6i$$

also $a_2 + a_2' i = -2i$

$$P_3 + P_3' i = -2i(-1 + 3i) - 3 = 3 + 2i$$

$$Q_3 + Q_3' i = \frac{4 + 5i - (3 + 2i)^2}{-1 + 3i} = -2 + i$$

$$x_3 = \frac{5{,}28 + 3{,}09i}{-2 + i} = \frac{-7{,}47 - 11{,}46i}{5} = -1{,}49 - 2{,}2i$$

Hier bleibt der reelle Theil des Quotienten vorläufig unbestimmt. Erwägt man aber, dass wenn δ und δ' resp. um die Werthe z und z' zu klein wären, der absolute Werth 7,47 des Zählers sich um $2z - z'$ erhöhen würde, und dass diese Erhöhung ihr Maximum für $z = 0{,}01$ und $z' = 0$ erreicht; so kann jener Zähler höchstens um 0,02 wachsen, also höchstens $= 7{,}49$ werden. Da aber $\frac{7{,}49}{5} < 1\frac{1}{2}$ bleibt; so ist

$$a_3 + a_3' i = -1 - 2i$$

$$P_4 + P_4' i = (-1 - 2i)(-2 + i) - (3 + 2i) = 1 + i$$

$$Q_4 + Q_4' i = \frac{4 + 5i - (1 + i)^2}{-2 + i} = -1 - 2i$$

$$x_4 = \frac{3{,}28 + 2{,}09i}{-1 - 2i} = \frac{-7{,}46 + 4{,}47i}{5} = -1{,}49 + 0{,}8i$$

Auch hier findet man, dass der Zähler 7,46 höchstens auf 7,48 steigen kann. Es ist also

$$a_4 + a_4' = -1 + i$$

$$P_5 + P_5' i = (-1 + i)(-1 - 2i) - (1 + i) = 2$$

$$Q_5 + Q_5' i = \frac{4 + 5i - 2^2}{-1 - 2i} = -2 - i$$

Da $a_4 + a_4' i = -(a_0 + a_0' i)$, $P_4 + P_4' i = P_0 + P_0' i$, $Q_4 + Q_4' i = -(Q_0 + Q_0' i)$ ist; so sieht man ohne weitere Rechnung ein, dass die Grössen $P + P'i$ von den Zeigern 4, 5, 6,... genau gleich denen von den Zeigern 0, 1, 2,... sind, während die Grössen $Q + Q'i$ und $a + a'i$ von den Zeigern 4, 5, 6,... das Entgegengesetzte der betreffenden Grössen von den Zeigern 0, 1, 2,... sein werden, sodass also die Gesammtheit dieser Grössen vom Zeiger 0 an eine achtgliederige Periode bildet.

Hiernach hat man für $K = \frac{\sqrt{4 + 5i} + 1 + i}{1 + 2i}$ folgende Entwickelung

n	$P_n + P_n' i$	$Q_n + Q_n' i$	$a_n + a_n' i$	$M_n + M_n' i$	$N_n + N_n' i$
-2				0	1
-1		$2 - i$		1	0
0	$1 + i$	$1 + 2i$	$1 - i$	$1 - i$	1
1	2	$2 + i$	$2 - i$	$2 - 3i$	$2 - i$
2	3	$-1 + 3i$	$-2i$	$-5 - 5i$	$-1 - 4i$
3	$3 + 2i$	$-2 + i$	$-1 - 2i$	$-7 + 12i$	$-5 + 5i$
4	$1 + i$	$-1 - 2i$	$-1 + i$	$-10 - 24i$	$-1 - 14i$
5	2	$-2 - i$	$-2 + i$	$37 + 50i$	$11 + 32i$
6	3	$1 - 3i$	$2i$	$-110 + 50i$	$-65 + 8i$
7	$3 + 2i$	$2 - i$	$1 + 2i$	$-173 - 120i$	$-70 - 90i$
8	$1 + i$	$1 + 2i$	$1 - i$	$-403 + 103i$	$-225 - 12i$
		etc.	etc.	etc.	

VII. Wenn die Determinante D kein vollständiges Quadrat einer ganzen Zahl ist, wird die vorstehende Kettenbruchsentwickelung von K **unendlich** sein, und es wird sich durch die sukzessiven Näherungsbrüche jeder Grad der Annäherung an den wahren Werth von K erreichen lassen.

Wenn dagegen die Determinante D ein vollständiges Quadrat ist, was sich sofort aus der Berechnung der rechten Seite der Gl. (4) ergibt, wird die Entwickelung eine endliche Länge besitzen, indem die Quotienten diejenigen Werthe annehmen, welche sich bei der gewöhnlichen Kettenbruchsentwickelung der rationalen Grösse K herausstellen. Dieser Fall bildet die Verallgemeinerung der in §. 82 ff. behandelten Spezialität, worin es sich um eine reelle quadratische Determinante handelt.

Wäre z. B. $K=\frac{\sqrt{-5-12i}+4-2i}{8+3i}$ gegeben; so hätte man nach Gl. (4)

$$\sqrt{-5-12i}=\sqrt{\frac{1}{2}(\sqrt{169}-5)}-\sqrt{\frac{1}{2}(\sqrt{169}+5)}\,.\,i$$

$$=\sqrt{4}-\sqrt{9}\,.\,i=2-3i$$

also $K=\frac{6-5i}{8+3i}$.

Im Übrigen bilden sich auch in diesem Falle die Grössen P und Q genau nach der früheren Regel. Der letzte Werth von P ist $=\sqrt{D}$ und der von $Q=0$.

Der in §. 94 betrachtete Fall, wo die Determinante eine negative reelle Zahl $-D$ ist, erfordert jetzt offenbar keine besondere Behandlung. Ist D ein vollkommenes Quadrat d^2; so ist es auch $-D=(di)^2$ und man erhält eine endliche Entwickelung. Unter entgegengesetzten Umständen wird die Entwickelung unendlich; dieselbe führt aber durch das gegenwärtige allgemeinere Verfahren nicht zu der in §. 94 bezeichneten zweigliederigen Periode mit annullirten Quotienten. Die Formel (4) ergibt für diesen Fall einfach

$$\sqrt{-D}=\sqrt{D}\,.\,i \tag{15}$$

VIII. Entwickeln wir als Beispiel die schon in §. 94 untersuchte Grösse

$$K=\frac{\sqrt{-8}-10}{27}$$

worin $D+D'i=-8$, $P_0+P_0'i=-10$, $Q_0+Q_0'i=27$, also $Q_{-1}+Q'_{-1}i=\frac{-8-(-10)^2}{27}=-4$ ist; so hat man zuvörderst nach Gl. (15) mit einer Annäherung auf Hundertstel

$$\sqrt{-8}=\sqrt{8}\,.\,i=2{,}82\ldots i$$

also $\delta+\delta'i=2{,}82i$, sodass $\delta=0$ und $\delta'=2{,}82$ ist. Hierdurch wird

$$K=x_0=\frac{-10+2{,}82i}{27}=-0{,}2+0{,}1i$$

also $a_0+a_0'i=0$

Hieraus folgt nach Gl. (1) und (2)

$$P_1+P_1'i=0\,.\,27-(-10)=10$$

$$Q_1+Q_1'i=\frac{-8-10^2}{27}=-4$$

$$x_1=\frac{10+2{,}82i}{-4}=-2{,}5-0{,}7i$$

also, da der reelle Theil von x_1 genau $= -2{,}5$ ist; sodass man ebenso gut $a_1 = -2$, wie auch $a_1 = -3$ nehmen kann,

$$a_1 + a_1'i = -2 - i$$

$$P_2 + P_2'i = (-2 - i)(-4) - 10 = -2 + 4i$$

$$Q_2 + Q_2'i = \frac{-8 - (-2 + 4i)^2}{-4} = -1 - 4i$$

$$x_2 = \frac{-2 + 6{,}82i}{-1 - 4i} = \frac{-25{,}28 - 14{,}82i}{17} = -1{,}48 - 0{,}8i$$

also $a_2 + a_2'i = -1 - i$

$$P_3 + P_3'i = (-1 - i)(-1 - 4i) - (-2 + 4i) = -1 + i$$

$$Q_3 + Q_3'i = \frac{-8 - (-1 + i)^2}{-1 - 4i} = -2i$$

$$x_3 = \frac{-1 + 3{,}82i}{-2i} = \frac{-7{,}64 - 2i}{4} = -1{,}9 - 0{,}5i$$

also, da der imaginäre Theil von x_3 genau $= -0{,}5i$ ist

$$a_3 + a_3'i = -2$$

$$P_4 + P_4'i = -2(-2i) - (-1 + i) = 1 + 3i$$

$$Q_4 + Q_4'i = \frac{-8 - (1 + 3i)^2}{-2i} = 3$$

$$x_4 = \frac{1 + 5{,}82i}{3} = 0{,}3 + 1{,}9i$$

also $a_4 + a_4'i = 2i$

$$P_5 + P_5'i = 2i \,.\, 3 - (1 + 3i) = -1 + 3i$$

$$Q_5 + Q_5'i = \frac{-8 - (-1 + 3i)^2}{3} = -2i$$

$$x_5 = \frac{-1 + 5{,}82i}{-2i} = -2{,}9 - 0{,}5i$$

und da der imaginäre Theil von x_5 genau $= 0{,}5$ ist,

$$a_5 + a_5'i = -3$$

$$P_6 + P_6'i = -3(-2i) - (-1 + 3i) = 1 + 3i$$

$$Q_6 + Q_6'i = \frac{-8 - (1 + 3i)^2}{-3} = 2i$$

$$x_6 = \frac{1 + 5{,}82i}{2i} = 2{,}9 - 0{,}5i$$

und da der imaginäre Theil von x_6 genau $= -5i$ ist,

$$a_6 + a_6'i = 3$$

$$P_7 + P_7'i = 3(2i) - (1 + 3i) = -1 + 3i$$

$$Q_7 + Q_7'i = \frac{-8-(-1+3i)^2}{2i} = 3$$

$$x_7 = \frac{-1+5{,}82i}{3} = -0{,}3+1{,}9i$$

also $a_7 + a_7'i = 2i$

$$P_8 + P_8'i = 2i\,.\,3 - (-1+3i) = 1+3i$$

$$Q_8 + Q_8'i = \frac{-8-(1+3i)^2}{2i} = -3$$

$$x_8 = \frac{1+5{,}82i}{-3} = -0{,}3-1{,}9i$$

also $a_8 + a_8'i = -2i$

Da $a_8 + a_8'i = -(a_4 + a_4'i)$, $P_8 + P_8'i = P_4 + P_4'i$, $Q_8 + Q_8'i = -(Q_4 + Q_4'i)$ ist; so erkennt man, dass die Grössen $P + P'i$ von den Zeigern 8, 9... gleich denen von den Zeigern 4, 5..., und dass die Grössen $Q + Q'i$ und $a + a'i$ von den Zeigern 8, 9... das Entgegengesetzte der betreffenden Grössen von den Zeigern 4, 5... sind, dass also vom Zeiger 4 an eine achtgliederige Periode eintritt. Der Anfang der Kettenbruchsentwickelung ist

n	$P_n + P_n'i$	$Q_n + Q_n'i$	$a_n + a_n'i$	$M_n + M_n'i$	$N_n + N_n'i$
-2				0	1
-1		-4		1	0
0	-10	27	0	0	1
1	10	-4	$-2-i$	1	$-2-i$
2	$-2+4i$	$-1-4i$	$-1-i$	$-1-i$	$2+3i$
3	$-1+i$	$-2i$	-2	$3+2i$	$-6-7i$
4	$1+3i$	3	$2i$	$-5+5i$	$16-9i$
5	$-1+3i$	$-2i$	-3	$18-13i$	$-54+20i$
6	$1+3i$	$2i$	3	$49-34i$	$-146+51i$
7	$-1+3i$	3	$2i$	$86+85i$	$-156-272i$
8	$1+3i$	-3	$-2i$	$219-206i$	$-690+363i$
9	$-1+3i$	$2i$	3	etc.	
10	$1+3i$	$-2i$	-3		
11	$-1+3i$	-3	$-2i$		
12	$1+3i$	3	$2i$		
	etc.				

IX. Als ferneres Beispiel fügen wir noch die Entwickelung von $K = \sqrt{i}$ hinzu, indem wir darauf aufmerksam machen, dass die Determinante i kein vollkommenes Quadrat ist. Hier hat man $D + D'i = i$, $P_0 + P_0'i = 0$, $Q_0 + Q_0'i = 1$, also $Q_{-1} + Q'_{-1}i = i$. Bei einer Annäherung bis auf Hundertstel ist nach Gl. (4)

$$\sqrt{i} = \sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2}}\,.\,i = 0{,}70\ldots + 0{,}70\ldots i$$

also $\delta + \delta' i = 0{,}7 + 0{,}7i$ oder $\delta = 0{,}7$, $\delta' = 0{,}7$. Hierdurch wird

$$K = x_0 = \frac{0{,}7 + 0{,}7i}{1} = 0{,}7 + 0{,}7i$$

also $a_0 + a_0' i = 1 + i$

$$P_1 + P_1' i = (1 + i) . 1 - 0 = 1 + i$$

$$Q_1 + Q_1' i = \frac{i - (1 + i)^2}{1} = - i$$

$$x_1 = \frac{1{,}7 + 1{,}7i}{-i} = -1{,}7 + 1{,}7i$$

also $a_1 + a_1' i = -2 + 2i$

$$P_2 + P_2' i = (-2 + 2i)(-i) - (1 + i) = 1 + i$$

$$Q_2 + Q_2' i = \frac{i - (1 + i)^2}{-i} = 1$$

$$x_2 = \frac{1{,}7 + 1{,}7i}{1} = 1{,}7 + 1{,}7i$$

also $a_2 + a_2' i = 2 + 2i$

$$P_3 + P_3' i = (2 + 2i)1 - (1 + i) = 1 + i = P_1 + P_1' i$$

$$Q_3 + Q_3' i = \frac{i - (1 + i)^2}{1} = - i = Q_1 + Q_1' i$$

$$x_3 = x_1$$

Hiernach ist die Entwickelung von $K \doteq \sqrt{i}$ vom Zeiger 1 an zweigliederig und man hat

n	$P_n + P_n' i$	$Q_n + Q_n' i$	$a_n + a_n' i$	$M_n + M_n' i$	$N_n + N_n' i$
-2				0	1
-1		i		1	0
0	0	1	$1 + i$	$1 + i$	1
1	$1 + i$	$-i$	$-2 + 2i$	-3	$-2 + 2i$
2	$1 + i$	1	$2 + 2i$	$-5 - 5i$	-7
3	$1 + i$	$-i$	$-2 + 2i$	17	$12 - 12i$
4	$1 + i$	1	$2 + 2i$	$29 + 29i$	41
		etc.	etc.	etc.	

Wir bemerken noch, dass sich die Entwickelung von $K = \sqrt{-i}$ aus der vorstehenden ergibt, wenn man darin überall $-i$ an die Stelle von i schreibt, die reellen Zahlen aber sämmtlich ungeändert lässt.

§. 201. *Periodizität und sonstige wichtige Eigenschaften der vorstehenden Kettenbruchsentwickelung. — Minimum von P und Q.*

I. Wir wollen jetzt zeigen, dass die vorstehende Kettenbruchsentwickelung K, wenn sie unendlich ist, also wenn die

Determinante keinen quadratischen Werth hat, stets periodisch sein wird.

Bezeichnen wir den bei der Division mit $Q_n + Q_n' i$ in $\sqrt{D + D' i} + P_n + P_n' i$ verbleibenden Rest mit $R_n + R_n' i$; so haben wir

$$(1) \qquad x_n = \frac{\sqrt{D + D' i} + P_n + P_n' i}{Q_n + Q_n' i} = a_n + a_n' i + \frac{R_n + R_n' i}{Q_n + Q_n' i}$$

Zur Abkürzung wollen wir schreiben

$$D + D' i = d e^{\delta i}, \qquad P_n + P_n' i = p e^{\varphi i}, \qquad Q_n + Q_n' i = q e^{\psi i},$$
$$R_n + R_n' i = r e^{\chi i}, \qquad a_n + a_n' i = a e^{\alpha i}$$

sodass $d = \sqrt{D^2 + D'^2}$, $p = \sqrt{P_n^2 + P_n'^2}$ etc. die absoluten Werthe der betreffenden Grössen darstellen.

Da hier immer ein mit absolut kleinsten Resten entwickelter Kettenbruch vorausgesetzt wird; so muss der absolute Werth jeder Grösse x_n, deren Zeiger > 0 ist, $\geqq \sqrt{2}$ sein, während immer, auch für den Zeiger 0 der absolute Werth des Restbruches $\leqq \frac{1}{\sqrt{2}}$ sein muss. Nun hat man

$$x_n = \frac{\sqrt{d e^{\delta i}} + p e^{\varphi i}}{q e^{\psi i}} = \frac{\sqrt{d}\, e^{\frac{\delta}{2} i} + p e^{\varphi i}}{q e^{\psi i}}$$

$$= \frac{\left(\sqrt{d} \cos\frac{\delta}{2} + p \cos\varphi\right) + \left(\sqrt{d} \sin\frac{\delta}{2} + p \sin\varphi\right) i}{q e^{\psi i}}$$

Folglich ist der absolute Werth von x^n

$$(2) \qquad \frac{\sqrt{d + p^2 + 2\sqrt{d}\, p \cos\left(\frac{\delta}{2} - \varphi\right)}}{q} \geqq \sqrt{2}$$

Dieser Werth erreicht sein Maximum für $\cos\left(\frac{\delta}{2} - \varphi\right) = 1$; Demnach ist

$$\frac{\sqrt{d + p^2 + 2\sqrt{d}\, p}}{q} = \frac{\sqrt{d} + p}{q} \geqq \sqrt{2} \qquad \text{oder}$$

$$(3) \qquad q \leqq \frac{\sqrt{d} + p}{\sqrt{2}}$$

und wegen des Restbruches hat man $\frac{r}{q} \leqq \frac{1}{\sqrt{2}}$, mithin

$$(4) \qquad r \leqq \frac{q}{\sqrt{2}} \leqq \frac{\sqrt{d} + p}{2}$$

Bezeichnen wir die Grössen vom nächstfolgenden Zeiger $n+1$ dadurch, dass wir den vorstehenden einen Index zufügen, so haben wir nach §. 200 Gl. (1)

(5) $$p_1 e^{\varphi_1 i} = aqe^{(\alpha+\psi)i} - pe^{\varphi i}$$

Nach Gl. (1) ist aber auch

(6) $$aqe^{(\alpha+\psi)i} - pe^{\varphi i} = \sqrt{de^{\delta i}} - re^{\lambda i}$$

folglich hat man auch

(7) $$p_1 e^{\varphi_1 i} = \sqrt{de^{\delta i}} - re^{\lambda i}$$

Hieraus leuchtet ein, dass man jedenfalls

(8) $$p_1 \leqq \sqrt{d} + r$$

d. i. wegen der Beziehung (4)

(9) $$p_1 \leqq \frac{3\sqrt{d}+p}{2}$$

Die beiden Beziehungen (3) und (9) beweisen die Periodizität. Denn ist $p > 3\sqrt{d}$; so wird nach (9) $p_1 \leqq p$. Ist dagegen $p < 3\sqrt{d}$; so bleibt nach (9) auch $p_1 \leqq 3\sqrt{d}$. Demnach muss im Laufe der Rechnung der absolute Werth der Grössen $P+P'i$ unter den Werth $3\sqrt{d}$ herabsinken, und kann sich von der Stelle, wo Dies zuerst geschieht, nicht wieder über $3\sqrt{d}$ erheben. Dadurch sind die ganzen Zahlen P und P' in gewisse Gränzen eingeschlossen, indem man von der fraglichen Stelle an

(10) $$\sqrt{P^2+P'^2} \leqq 3\sqrt{\sqrt{D^2+D'^2}} \text{ oder } (P^2+P'^2)^2 \leqq 81(D^2+D'^2)$$

hat.

Die Werthe von q müssen von dieser Stelle an wegen der Beziehung (3) $q \leqq \frac{4\sqrt{d}}{\sqrt{d}}$ oder $\leqq 2\sqrt{2\sqrt{d}}$ sein. Demnach sind auch die ganzen Zahlen Q und Q' von jener Stelle an in die durch

(11) $$\sqrt{Q^2+Q'^2} \leqq 2\sqrt{2\sqrt{\sqrt{D^2+D'^2}}} \text{ oder } (Q^2+Q'^2)^2 \leqq 64(D^2+D'^2)$$

bezeichneten Gränzen eingeschlossen.

Hieraus folgt die endliche Wiederkehr zweier Grössen wie $P_n + P_n'i$ und $Q_n + Q_n'i$, also die Wiederkehr des Werthes x_n an einer späteren Stelle und daraus die Periodizität der Entwickelung.

II. Es leuchtet ein, dass für die periodischen Kettenbrüche mit komplexen Quotienten auch die Reduktionsformel des §. 58, sowie die Formeln der §§. 67 und 68 gültig sind. Dabei ist es hier wie dort statthaft, dass sich unter den Quotienten auch willkürliche Zahlen befinden. Allemal jedoch, wo die

Konvergenz des Kettenbruches eine nothwendige Bedingung ist, muss die Entwickelung nach dem Prinzipe **der absolut kleinsten Reste** geschehen sein.

Ähnlich wie in §. 70 gelangt man auch zu dem Schlusse, dass alle anfangs willkürlichen Entwickelungen von K, wenn sie von irgend einer Stelle an mit absolut kleinsten Resten fortgesetzt werden, früher oder später sämmtlich **Ein und dieselbe Periode** annehmen.

Ferner ist klar, dass die in §. 73 beschriebene **Kombination** zweier Kettenbrüche auch hier, wo es sich um komplexe Quotienten handelt, ausgeführt werden kann, insofern die dazu erforderlichen Bedingungen erfüllt sind. Diese Bedingungen sind bekanntlich Gleichheit der Perioden oder des Schlusses beider Entwickelungen bei gleicher Determinante.

III. Es ist noch von besonderer Wichtigkeit, den absolut kleinsten Werth q von $Q+Q'i$ zu untersuchen, welcher sich durch angemessen gewählte Quotienten erreichen lässt.

Bei der Entwickelung mit absolut kleinsten Quotienten haben wir vorhin gesehen, dass der numerische Werth einer jeden periodischen Grösse $Q+Q'i$ der Bedingung $q \leqq 2\sqrt{2}\sqrt{d}$ entsprechen müsse. Es ist klar, dass dieser Werth auch $<d$ ist; sobald man $d>8$ hat. Wenn also der absolute Werth $\sqrt{D^2+D'^2}$ der Determinante **grösser** als 8 ist, wird **der absolute Werth einer jeden periodischen Grösse** $Q+Q'i$, d. i. $\sqrt{Q^2+Q'^2}<\sqrt{D^2+D'^2}$, **also kleiner als der absolute Werth der Determinante sein.**

Wenn jedoch der absolute Werth der Determinante **kleiner** oder **gleich** 8 ist, lässt sich aus dem Vorstehenden nicht ohne Weiteres schliessen, dass sich in der Periode eine Grösse $Q+Q'i$ antreffen werde, welche absolut kleiner, als die Determinante sei.

IV. Zu einem solchen Werthe von $Q+Q'i$, welcher absolut kleiner als die Determinante ist, kann man aber stets gelangen, wenn man im Sinne des §. 69 eine Entwickelung vornimmt, wobei die Quotienten $a+a'i$ den rationalen Theil der Ausdrücke x_n, also die Grösse $\frac{P+P'i}{Q+Q'i}$ möglichst vollständig, d. h. unter Zurücklassung absolut kleinster Reste, erschöpfen.

Denn setzt man unter diesen Umständen

$$(12)\qquad \frac{pe^{\varphi i}}{qe^{\psi i}} = ae^{\alpha i} + \frac{re^{\chi i}}{qe^{\psi i}},\ \text{also}\ pe^{\varphi i} = aqe^{(\alpha+\psi)i} + re^{\chi i}$$

so muss $\frac{r}{q} \leqq \frac{1}{\sqrt{2}}$ oder $r \leqq \frac{q}{\sqrt{2}}$ sein, und man hat für das nächstfolgende p nach Gl. (5) und (12)

(13) $$p_1 e^{\varphi_1 i} = -r e^{\chi i} = r e^{(\pi+\chi i)}$$

(14) $$p_1 = r \leqq \frac{q}{\sqrt{2}}$$

Wäre nun nicht gleichzeitig auch $p_1 \leqq \frac{q_1}{\sqrt{2}}$, sondern $> \frac{q_1}{\sqrt{2}}$; so hat man für das jetzt folgende p, wegen (14), $p_2 = r_1 \leqq \frac{q_1}{\sqrt{2}}$, also $p_2 < p_1$; folglich wäre dann das spätere p absolut kleiner, als das vorhergehende. Da dies Kleinerwerden eine Gränze null hat, welche in der That kleiner ist, als jeder Werth von der Form $\frac{q}{\sqrt{2}}$; so ist klar, dass endlich einmal gleichzeitig

(15) $$p_1 \leqq \frac{q}{\sqrt{2}} \text{ und auch } \leqq \frac{q_1}{\sqrt{2}}$$

oder

(16) $$\sqrt{2}p_1 \leqq q \text{ und auch } \leqq q_1$$

werden muss. Für diese Werthe hat man also

(17) $$qq_1 \geqq 2p_1^2$$

Nun ist nach der Grundformel §. 200, Gl. (2)

$$de^{\delta i} - (p_1 e^{\varphi_1 i})^2 = q e^{\psi i} q_1 e^{\psi_1 i}, \text{ d. i.}$$

(18) $$de^{\delta i} - p_1^2 e^{2\varphi_1 i} = qq_1 e^{(\psi+\psi_1)i}$$

also entschieden

(19) $$d + p_1^2 \geqq qq_1$$

mithin wegen (17)

$$d + p_1^2 \geqq 2p_1^2, \text{ folglich}$$

(20) $$p_1^2 \leqq d \text{ oder } p_1 \leqq \sqrt{d}$$

und demnach auch wegen (19)

(21) $$qq_1 \leqq 2d$$

folglich

(22) $$\text{entweder } q \text{ oder } q_1 \leqq \sqrt{2d}$$

Es ist also immer möglich, in der Entwickelung von K eine Grösse $P+P'i$ herzustellen, für welche nach (20)

(23) $$\sqrt{P^2+P'^2} \leqq \sqrt{\sqrt{D^2+D'^2}} \text{ oder } (P^2+P'^2)^2 \leqq D^2+D'^2$$

ist, während für die zugehörige oder die nächstfolgende Grösse $Q+Q'i$ nach (22)

(24) $\sqrt{Q^2+Q'^2} \leqq \sqrt{2\sqrt{D^2+D'^2}}$ oder $(Q^2+Q'^2)^2 \leqq 4(D^2+D'^2)$ ist.

V. Man kann auch behaupten, dass der absolute Werth q der zuletzt erwähnten Grösse $Q+Q'i$ stets kleiner, als der absolute Werth d der Determinante $D+D'i$, dass also $q<d$ sei, und dass nur dann tiefstens $q=d$ werde, wenn man $d=1$ hat. Denn allgemein wird die rechte Seite der Ungleichheit (22) oder $\sqrt{2d}<d$ sein, wenn man $d>2$, also in allen den Fällen, wo der numerische Werth der Determinante, d. i. $\sqrt{D^2+D'^2}>2$ oder das Quadrat davon $D^2+D'^2>4$ ist.

Was aber die hierunter nicht enthaltenen Fälle betrifft, in welchen $d\leqq 2$ ist; so kann für dieselben die Determinante $D+D'i$ nur Eine der vier Formen 0, i^m, $(1+i)i^m$, $2i^m$ haben. Hiervon sind 0, ± 1, $\pm 2i$ vollkommene Quadrate, welche zu einer endlichen Entwickelung und schliesslich zum Werthe $q=0$ führen, also die gewünschte Eigenschaft besitzen.

Keine Quadrate sind dagegen $\pm i$, $(1+i)i^m$, ± 2, welche wir einzeln als Determinanten betrachten wollen.

Wenn $D+D'i=de^{\delta i}=\pm i$, also $d=1$ ist; so muss nach (20)

$$p_1^2\leqq 1 \text{ also } =0 \text{ oder } 1\text{, folglich } p_1e^{\varphi_1 i}=0,\ \pm 1,\ \pm i$$
$$\text{und } (p_1e^{\varphi_1 i})^2=0,\quad 1,\ -1$$

werden. Da man nun wegen der allgemeinen Gl. (18) stets

$$qe^{\psi i}q_1e^{\psi_1 i}=\pm i-(p_1e^{\varphi_1 i})^2$$

ist; so ist klar, dass wenn das zweite Glied auf der rechten Seite nur den Werth 0, 1 oder -1 haben kann, diese rechte Seite nur $=\pm i$ oder $=(1+i)i^m$ sein kann, dass also, da $1+i$ eine Primzahl ist, Eine der beiden Grössen $qe^{\psi i}$ oder $q_1e^{\psi_1 i}=i^n$, folglich entweder q oder $q_1=1$ sein muss, was zu beweisen war.

Wenn $D+D'i=de^{\delta i}=(1+i)i^m$, also $d=\sqrt{2}$ ist; so muss nach (20)

$$p_1^2\leqq\sqrt{2}\text{, also } =0 \text{ oder } 1\text{, folglich } p_1e^{\varphi_1 i}=0,\ \pm 1,\ \pm i$$
$$\text{und } (p_1e^{\varphi_1 i})^2=0,\quad 1,\ -1$$

werden. Die Gl. (18) ist hier

$$qe^{\psi i}q_1e^{\psi_1 i}=(1+i)i^m-(p_1e^{\varphi_1 i})^2$$

Da nun das zweite Glied auf der rechten Seite nur $=0$, 1 oder -1 sein kann; so kann diese rechte Seite nur von Einer der drei Formen i^n, $(1+i)i^n$, $(2+i)i^n$ sein. In jedem Falle muss

aber, da Dies sämmtlich Primzahlen sind, entweder $qe^{\psi i}$ oder $q_1 e^{\psi_1 i} = i^r$, folglich entweder q oder $q_1 = 1$ sein, was zu beweisen war.

Wenn endlich $D + D'i = de^{\delta i} = \pm 2$, also $d = 2$ ist; so muss nach (20)

$$p_1^2 \leqq 2, \text{ also } = 0, 1, 2, \text{ folglich } p_1 e^{\varphi_1 i} = 0, \quad i^m, \quad (1+i)i^m$$
$$\text{und } (p_1 e^{\varphi_1 i})^2 = 0, \ \pm 1, \quad \pm 2i$$

werden. Die Gl. (18) gibt hier

$$qe^{\psi i} q_1 e^{\psi_1 i} = \pm 2 - (p_1 e^{\varphi i})^2$$

Nimmt man das zweite Glied auf der rechten Seite $= 0$ oder $= \pm 1$; so wird diese Seite $= \pm 2, \ \pm 1, \ \pm 3$. Da $2 = (1+i)^2 i^3$ und 3 eine Primzahl ist; so ist klar, dass unter diesen Umständen $qe^{\psi i}$ oder $q_1 e^{\psi_1 i}$ entweder $= i^n$ oder $= (1+i)i^n$ also in beiden Fällen absolut kleiner, als die Determinante sein muss, was zu beweisen war.

Nimmt man das zweite Glied auf der rechten Seite $= \pm 2i$; so wird dieselbe $= 2(1+i)i^n = (1+i)^3 i^r$. Alsdann muss aber $qe^{\psi i}$ oder $q_1 e^{\psi_1 i} = (1+i)i^s$, also absolut kleiner als die Determinante sein, was zu beweisen war.

Man kann also unter allen Umständen bewirken, dass wenn die Determinante absolut > 1 ist, eine Grösse $Q + Q'i = qe^{\psi i}$ entsteht, welche absolut kleiner ist, als die Determinante. In dem besonderen Falle, wo die Determinante absolut $= 1$ und kein Quadrat, also $= \pm i$ ist; kann stets eine Grösse $Q + Q'i = i^m$ von demselben absoluten Werthe erzielt werden. Da nun aber jeder Ausdruck von der Form

$$x^n = \frac{\sqrt{\pm i} + P + P'i}{i^m}$$

in der nächsten Entwickelungsstufe für

$$a_n + a_n' i = \frac{P + P'i}{i^m} = Pi^{3m} + P'i^{3m+1}$$

das Glied

$$x_{n+1} = \frac{\sqrt{\pm i} + 0}{\pm i^{1-m}}$$

erzeugt, und Eine der beiden Grössen i^m oder i^{1-m} jedenfalls reell, also $= \pm 1$ ist; so ist klar, dass sich bei der Determinante $\pm i$ immer eine Grösse $Q + Q'i = \pm 1$ erzielen lässt, welche ein vollkommenes Quadrat ist.

VI. Die Möglichkeit, die Grössen p_1, q, q_1 auf gewisse Minima zu bringen, gewährt ähnlich wie in §. 124 die Mittel zur Reduktion der quadratischen Formen in komplexen Zahlen.

§. 202. *Auflösung der unbestimmten Gleichungen vom zweiten Grade mit zwei Unbekannten in komplexen ganzen Zahlen, wenn die linke Seite eine homogene Form ist. — Aufsuchung der durch q theilbaren Zahlen von der Form D — p².*

I. Die Betrachtung des §. 74 ist auch hier, wo es sich um komplexe Grössen handelt, anwendbar. Demnach kann die Auflösung der unbestimmten Gleichung

(1) $$ax^2 - 2bxy - cy^2 = k$$

worin die Koeffizienten a, b, c, k beliebige komplexe Zahlen sein können und die Unbekannten x, y in allgemeinster Form gesucht werden, nach den im fünften Abschnitte, §. 100 entwickelten Prinzipien geschehen.

Wäre in einer gegebenen Gleichung der Koeffizient xy nicht paar; so kann man, um Dies zu erreichen, die Gleichung resp. mit $1 + i$ oder mit 2 multipliziren, jenachdem jener Koeffizient vollkommen unpaar ist oder nicht.

Man bildet hier wie dort die Grösse $K = \frac{\sqrt{D} + P_0}{Q_0}$ und entwickelt sie in einen Kettenbruch mit absolut kleinsten Resten.

Jetzt untersucht man, ob es ganze (im Allgemeinen komplexe) Werthe p gibt, für welche $D - p^2$ durch k theilbar wird.

Gibt es solche Werthe nicht; so ist die Aufgabe unmöglich. Gibt es deren aber; so hat man für irgend Einen derselben die Grösse $K' = \frac{\sqrt{D} + p}{k}$ in einen Kettenbruch mit absolut kleinsten Resten zu entwickeln. Stimmt die Periode desselben mit der von K überein; so kann K und K' kombinirt werden, und Dies führt, wenn die Determinante D kein vollkommenes Quadrat ist, hier wie dort zu einer unendlichen, sonst aber zu einer endlichen Menge von Auflösungen. Von der Bedingung, dass bei den zu kombinirenden Entwickelungen die Zeigersumme der übereinstimmenden Glieder eine paare Zahl sei, kann hier abstrahirt werden, wenn man die sich für x und y ergebenden Werthe nöthigenfalls mit i multiplizirt, wodurch die rechte Seite der Gl. (1) $= -k$ wird.

Bei der Untersuchung der quadratischen Faktoren von k hat man die vollständige Zerlegung dieser Zahl in ihre kom-

plexen Faktoren zu berücksichtigen, auch zu beachten, dass $+1=(-1)^2$ und auch $=-(i)^2$, und dass $-1=(i)^2$ ist.

II. Nach dem Vorstehenden kommt es also darauf an, Zahlen p zu finden, für welche $I=D-p^2$ durch eine gegebene Zahl q theilbar wird.

Zuvörderst ist klar, dass wenn p ein gesuchter Werth ist, auch $-p$ ein solcher sein wird, dass man also, um auch die letzteren leicht zu bestimmen, nur die ersteren zu bestimmen braucht.

Alsdann leuchtet hier ebenso ein, wie in §. 75 ff., dass wenn p ein gesuchter Werth ist, auch $p+wq$ ein solcher ist, worin w eine willkürliche ganze, also im Allgemeinen komplexe Zahl darstellt. Demnach ist p der Vertreter einer unendlichen Gruppe ähnlicher Zahlen, welche in der Form $p+wq$ enthalten sind, indem man darin für w nach und nach alle denkbaren ganzen Zahlen setzt.

Man erkennt bald, dass es auch hier nur darauf ankommt, aus jeder verschiedenen unendlichen Gruppe dieser Art ein einziges Glied p zu kennen und in den Werth von K' zu substituiren. Jedes andere Glied liefert genau dieselben Auflösungen wie p.

Es entsteht nun die Frage nach den Gränzen, bis zu welchen man in dem Ausdrucke $I=D-p^2$ die Zahlen p in der komplexen Form wachsen zu lassen und die Theilbarkeit von I durch q zu untersuchen braucht, um von jeder selbstständigen Gruppe der Zahlen I, welche der Form

(2) $$I=D-(p+wq)^2=D-P^2$$

entspricht, mit Gewissheit Ein Glied zu entdecken.

III. Diese Untersuchung wollen wir durch geometrische Konstruktion erledigen, um ein ferneres Beispiel von der Fruchtbarkeit des Situationskalkuls zu geben.

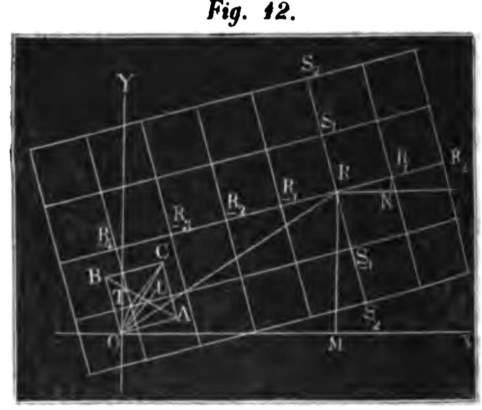
Um die komplexe Zahlform besser vor Augen zu führen; so sei $p+p'i$ irgend eine ganze Zahl, wodurch $I=D+D'i-(p+p'i)^2$ durch $q+q'i$ theilbar wird. Die einzelnen Glieder der zugehörigen Gruppe werden erhalten, wenn man statt $p+p'i$ irgend eine Zahl von der Form

(3) $$P+P'i=p+p'i+(w+w'i)(q+q'i)$$

nimmt. Es kommt jetzt darauf an, zu zeigen, dass, welches auch die Zahl $p+p'i$ sei, die Willkürliche $w+w'i$ stets so genommen werden kann, dass die Grösse $P+P'i$ innerhalb gewisser Gränzen zu liegen kommt, welche nur von $q+q'i$, nicht aber von $p+p'i$ abhängen.

Um die verschiedenen Werthe der Grösse $P+P'i$ geometrisch zu konstruiren; so sei in Fig. 12 O der Nullpunkt, OX die positiv reelle und OY die positiv imaginäre Axe. Statt Gl. (3) kann man schreiben

Fig. 12.



(4) $$P+P'i = p+p'i+w(q+q'i)+w'(q+q'i)i$$

Ist nun $OM=p$, $MR=p'$; so ist $(OR)=p+p'i$. Ist ferner in der Richtung der reellen Axe $RN=q$ und in der Richtung der imaginären $NR_1=q'$; so ist $(RR_1)=q+q'i$.

Jenachdem man $w=0,\ 1,\ 2\ldots$ setzt, ist resp.

$$(R),\ (RR_1),\ (RR_2)\ldots = 0,\ (q+q'i),\ 2(q+q'i)\ldots$$

Jenachdem man $w=0,\ -1,\ -2\ldots$ setzt, ist resp.

$$(R),\ (RR_{-1}),\ (RR_{-2})\ldots = 0,\ -(q+q'i),\ -2(q+q'i)\ldots$$

Ist RS_1 rechtwinklig auf RR_1 durch Drehung von rechts nach links aus RR_1 entstanden, und der Länge nach $RS_1=RR_1$; so hat man $(RS_1)=(q+q')i$, also jenachdem man $w'=0, 1, 2\ldots$ setzt, resp.

$$(R),\ (RS_1),\ (RS_2)\ldots = 0,\ (q+q'i)i,\ 2(q+q'i)i\ldots$$

und jenachdem man $w'=0,\ -1,\ -2\ldots$ setzt, resp.

$$(R),\ (RS_{-1}),\ (RS_{-2})\ldots = 0,\ -(q+q'i)i,\ -2(q+q'i)i\ldots$$

Dadurch also, dass man sowol die Grösse w, wie auch die Grösse w' zwischen positiven und negativen reellen ganzen Zahlen variiren lässt, gelangt man vom Punkte R aus in die verschiedenen Eckpunkte des verzeichneten quadratischen Netzes, z. B. in den Punkt T, für welchen man hat

$$(OT)=(OR)+(RT)=(OR)+(RR_{-4})+(R_{-4}T)$$
$$=p+p'i-4(q+q'i)-(q+q'i)i=(p+p'i)+(-4-i)(q+q'i)$$

sodass für diesen Punkt $w+w'i=-4-i$ und $P+P'i=(OT)$ ist.

Bei gehöriger Erweiterung des quadratischen Netzes, wovon R ein Eckpunkt ist, wird der Nullpunkt O in das Innere oder n den Umfang Eines jener Quadrate zu liegen kommen, und es leuchtet ein, dass für Einen der vier Eckpunkte des letzteren Quadrates die parallel zu den Richtungen

RR_1 und RS_1 gemessenen beiden Abstände vom Nullpunkte nicht grösser sein können, als die halbe Länge der Quadratseite $RR_1 = \sqrt{q^2 + q'^2}$. Es ist also jeder der fraglichen beiden Abstände $\leqq \frac{1}{2}\sqrt{q^2 + q'^2}$, d. h. kleiner oder gleich dem halben absoluten Werthe von $q + q'i$.

Tragen wir nun an den Nullpunkt ein den früheren gleiches und paralleles Quadrat $OACB$, sodass $(OA) = q + q'i$ und $(OB) = (q + q'i)i$ ist; so muss nothwendig Ein Eckpunkt T des mehrgenannten quadratischen Netzes in dieses Quadrat fallen. Es kann aber auch nur ein einziger solcher Punkt in das Innere dieses Quadrates fallen. Fielen zwei Netzpunkte darauf; so müssen dieselben beide im Umfange des Quadrates $OACB$ und zwar entweder parallel zu OA oder parallel zu OB einander gegenüber liegen. Fielen gar vier Netzpunkte auf das Quadrat $OACB$; so könnte Dies nur in den Eckpunkten des Letzteren geschehen.

Die verschiedenen zu untersuchenden Netze, von denen jedes durch seine Eckpunkte zu einer besonderen Gruppe von Zahlen I führt, unterscheiden sich, da ihnen sämmtlich die Grösse $q + q'i$ gemein ist, nur durch den Werth von $p + p'i$, also durch die Lage des Punktes R.

Untersuchen wir also alle in dem festen Quadrate $OACB$ liegenden Punkte, welche ganze Zahlen $(OT) = P + P'i$ darstellen; so ist ein jeder, welcher der Bedingung der Aufgabe entspricht, der Anfangspunkt eines selbstständigen Netzes und entspricht einer selbstständigen Gruppe von Zahlen I. Nur wenn ein solcher Punkt in eine Seitenlinie jenes Quadrates fiele, muss man schliessen, dass der gegenüber liegende keine neue Gruppe bedingt. Dasselbe gilt, wenn ein solcher Punkt in einen Eckpunkt des genannten Quadrates fällt, von den übrigen drei Eckpunkten.

Bei unserer Aufgabe kommt aber nicht der Werth von $P + P'i$ selbst, sondern der von $(P + P'i)^2$ in Betracht, sodass, wenn $P + P'i$ einen gesuchten Werth darstellt, auch $-P - P'i$ ein solcher ist, welcher der konjugirten Gruppe entspricht. Ist nun das Quadrat $OACB$ durch die Diagonale AB in zwei kongruente Dreiecke OAB und CAB getheilt und sind T und U zwei diametral einander korrespondirende Punkte, für welche CT gleich und parallel OU ist, von denen also der Eine in diesem und der andere in jenem Dreiecke liegt; so hat man, wenn man $(OU) = P + P'i$ setzt und beachtet, dass $(OC) = (1 + i)(q + q'i)$ ist,

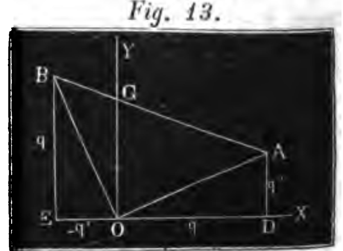
$$(OT) = (OC) + (CT) = (OC) - (OU), \quad \text{d. i.}$$
$$= (1 + i)(q + q'i) - (P + P'i)$$
$$= -(P + P'i) + (1 + i)(q + q'i)$$

Hieraus folgt, dass wenn es im Dreiecke CAB einen gesuchten Punkt gibt, es auch im Dreiecke OAB einen solchen geben wird, dass man also nur für die Punkte des letzteren Dreiecks zu untersuchen braucht, ob sich darunter solche finden, für welche $D + D'i - (P + P'i)^2$ durch $q + q'i$ theilbar wird.

Schliesslich hat man dann die gefundenen Werthe von $P + P'i$ auch mit entgegengesetztem Zeichen zu nehmen, wodurch die konjugirten Gruppen entstehen. Man findet leicht, dass wenn ein Punkt in irgend eine Seitenlinie OA, OB, AB des Dreiecks OAB fällt, nothwendig ein Punkt der konjugirten Gruppe in dieselbe Seitenlinie, und zwar gleich weit von der Mitte dieser Linie nach der entgegengesetzten Seite fallen muss. Von den in eine Seitenlinie fallenden Punkten braucht man also nicht auch noch die entgegengesetzten Werthe zu betrachten. Ausserdem erhellet, dass die Eckpunkte O, A, B immer nur eine einzige Gruppe bedingen würden.

Man kann auch die Notirung der Zahlen so vornehmen. Man notirt für alle vier Eckpunkte des Quadrats den Einen Zahlwerth 0 mit der Bemerkung, dass sich daraus keine konjugirte Reihe ergibt. Ferner notirt man für jede Mitte der drei Seiten des Dreiecks OAB, welche sich als Endpunkt einer ganzen Zahl herausstellt, den betreffenden Einen Zahlwerth mit derselben Bemerkung. Endlich nimmt man von den übrigen etwa in eine Seitenlinie des Dreiecks OAB fallenden Zahlen nur die in der Einen Hälfte liegenden. Diese letzteren Zahlen ergeben dann, ebenso wie die im Innern des Dreiecks OAB liegenden, durch Umkehrung des Zeichens auch konjugirte Gruppen.

IV. Die Aufsuchung der Punkte des Dreiecks OAB wird erleichtert, wenn man immer dafür sorgt, dass in dem Divisor $q + q'i$ die beiden Grössen q und q' positiv sind. Dies kann stets geschehen, indem man diesen Divisor nöthigenfalls mit i, i^2 oder i^3 multiplizirt, was auf die gesuchten Werthe von $P + P'i$ offenbar ohne Einfluss ist. Alsdann liegt OA stets im Quadranten XOY.



Fällt man in Fig. 13 von A und B die Perpendikel AD und BE auf die reelle Axe; so hat man $OD = q$, $DA = q'$, $OE = -q'$, $EB = q$. Die zur imaginären Axe parallelen Ordinaten der Punkte des Flächentheils OGB liegen zwischen denen der Linien OB und GB, und die Ordinaten der Punkte

des Flächentheils OGA liegen zwischen denen der Linien OA und GA. Nun hat man, wenn p irgend eine reelle Zahl bezeichnet, für den Vektor $p+p'i$ irgend eines Punktes

der Linie OB den Ausdruck (5) $p-\frac{q}{q'}pi$

» » OA » » (6) $p+\frac{q'}{q}pi$

» » BA » » (7) $p+\left(\frac{q^2+q'^2}{q+q'}+\frac{q'-q}{q+q'}p\right)i$

Jetzt substituirt man für p

in (5) alle reellen ganzen Zahlen von $-q'$ bis 0
» (6) » » » » » 0 bis q
» (7) » » » » » $-q'$ bis q

und sieht nach, welche komplexe ganze Zahlen es für jeden Werth von p gibt, und welche der Bedingung entsprechen; dass ihre imaginären Theile zwischen denen von (5) und (7), resp. von (6) und (7) liegen.

Wäre q oder $q'=0$; so hätte man nur resp. eine Kombination von (5) und (7) oder von (6) und (7) zu betrachten.

Hierdurch ergeben sich alle Zahlen von der Form $p+p'i$, für welche zu untersuchen ist, ob dadurch $I=D+D'i-(p+p'i)^2$ durch $q+q'i$ theilbar, oder ob

$$\frac{D+D'i-(p+p'i)^2}{q+q'i}=\frac{[D+D'i-(p+p'i)^2](q-q'i)}{q^2+q'^2}$$

eine ganze Zahl wird.

V. Als Beispiel zu Vorstehendem sei $D+D'i=-17+27i$, $q+q'i=5+8i$ gegeben, sodass also $-17+27i-(p+p'i)^2$ durch $5+8i$ theilbar werden soll. Die Ausdrücke (5), (6), (7) werden hier

(5) $p-\frac{5}{8}pi$

(6) $p+\frac{8}{5}pi$

(7) $p+\left(\frac{89}{13}+\frac{3}{13}p\right)i$

Lässt man die Grösse p in (5) von -8 bis 0, in (6) von 0 bis 5 und in (7) von -8 bis 5 variiren; so erhält man durch leichte, auf Additionen sich zurückführende Rechnungen

p	aus (5) p'	aus (6) p'	aus (7) p'	also in ganzen Zahlen $p' =$
-8	5		5	5
-7	$4\frac{3}{8}$		$5\frac{3}{13}$	5
-6	$3\frac{6}{8}$		$5\frac{6}{13}$	4, 5,
-5	$3\frac{1}{8}$		$5\frac{9}{13}$	4, 5,
-4	$2\frac{4}{8}$		$5\frac{12}{13}$	3, 4, 5,
-3	$1\frac{7}{8}$		$6\frac{2}{13}$	2, 3, 4, 5, 6
-2	$1\frac{2}{8}$		$6\frac{5}{13}$	2, 3, 4, 5, 6
-1	$\frac{5}{8}$		$6\frac{8}{13}$	1, 2, 3, 4, 5, 6
0	0	0	$6\frac{11}{13}$	0, 1, 2, 3, 4, 5, 6
1		$1\frac{3}{5}$	$7\frac{1}{13}$	2, 3, 4, 5, 6, 7.
2		$3\frac{1}{5}$	$7\frac{4}{13}$	4, 5, 6, 7
3		$4\frac{4}{5}$	$7\frac{7}{13}$	5, 6, 7
4		$6\frac{2}{5}$	$7\frac{10}{13}$	7
5		8	8	8

Diese 47 ganzen Werthe von $p+p'i$ sind auf die verlangte Eigenschaft zu prüfen. Im Umfange des Dreiecks OAB liegen davon drei, nämlich $-8+5i$, 0 und $5+8i$, und zwar liegen dieselben in den Ecken B, O, A. Erwiese sich also Einer von diesen drei Werthen als zulässig; so würden die anderen keine neuen Gruppen bedingen. Jeder andere zulässige Werth führt aber hier, wenn er mit entgegengesetztem Zeichen genommen wird, zu einer anderen und verschiedenen konjugirten Gruppe.

Die eben genannte Prüfung wird ausgeführt, indem man nachsieht, welche der vorstehenden Werthe von $p+p'i$ den Ausdruck

$$\frac{-17+27i-(p+p'i)^2}{5+8i} = \frac{-17-p^2+p'^2+(27-pp')i}{5+8i}$$
$$= \frac{131-5(p^2-p'^2)-16pp'}{89} + \frac{271+8(p^2-p'^2)-10pp'}{89}i$$

zu einer ganzen Zahl machen. Man findet, dass nur der einzige Werth $p+p'i=-1+2i$ dieser Bedingung genügt, indem der vorstehende Ausdruck hierfür $=2+3i$ wird. Die konjugirte Gruppe entspricht dem Werthe $p+p'i=1-2i$.

Hiernach ist allgemein

$$P+P'i=-1+2i+(w+w'i)(5+8i)=(-1+5w-8w') + (2+8w+5w')i$$

und

$$P+P'i=1-2i+(w+w'i)(5+8i)=(1+5w-8w') + (-2+8w+5w')i$$

eine ganze Zahl, welche der Aufgabe genügt.

Es wird noch darauf aufmerksam gemacht, dass man bei einer einigermaassen genauen Konstruktion die in dem Dreiecke *OAB* liegenden ganzen Zahlen auch durch Zeichnung ermitteln kann.

VI. Schliesslich bemerken wir, dass wenn relativ prime Faktoren bekannt sind, in welche sich die Zahl $q+q'i$ zerlegen lässt, man auch für jeden dieser Faktoren die Zahlen I aufsuchen und nach §. 79, III. verfahren kann. Auch lehrt eine Betrachtung wie in §. 80, dass wenn $q+q'i$ vollkommen prim ist, es nur eine einzige Gruppe der Zahlen I und die konjugirte derselben geben kann.

§. 203. ***Beispiel mit nicht quadratischer Determinante:***

$$(1+2i\ x^2-2(1+i)xy-(2-i)y^2=-2+5i$$

Hier ist $Q_0+Q_0'i=1+2i$, $P_0+P_0'i=1+i$, $Q_{-1}+Q_{-1}'i=2-i$, $D+D'i=(1+i)^2+(1+2i)(2-i)=4+5i$, also

$$K=\frac{\sqrt{4+5i}+1+i}{1+2i}$$

Die Entwickelung dieser Grösse ist in §. 200, VI. mitgetheilt.

Ferner hat man $K'=\dfrac{\sqrt{4+5i}+p+p'i}{-2+5i}$. Es sind also die durch $-2+5i$ theilbaren Zahlen von der Form $4+5i-(p+p'i)^2$ zu suchen. Damit im Divisor beide Theile positiv werden, setzen wir statt desselben die Zahl $(-2+5i)i^3=5+2i=q+q'i$. Demnach hat man statt der Ausdrücke (5), (6), (7) aus dem vorhergehenden Paragraphen

$$(5)\qquad p-\frac{5}{2}pi$$

$$(6)\qquad p+\frac{2}{5}pi$$

$$(7)\qquad p+\left(\frac{29}{7}-\frac{3}{7}p\right)i$$

Lässt man die Grösse p in (5) und (7) von -2 bis 0 und in (6) und (7) von 0 bis 5 variiren; so kommt

	aus (5)	aus (6)	aus (7)	also in ganzen Zahlen
p	p'	p'	p'	$p'=$
—2	5		5	5
—1	$2\frac{1}{2}$		$4\frac{4}{7}$	3, 4
0	0	0	$4\frac{1}{7}$	0, 1, 2, 3, 4
1		$\frac{2}{5}$	$3\frac{5}{7}$	1, 2, 3
2		$\frac{4}{5}$	$3\frac{2}{7}$	1, 2, 3
3		$1\frac{1}{5}$	$2\frac{6}{7}$	2
4		$1\frac{3}{5}$	$2\frac{3}{7}$	2
5		2	2	2

Aus diesen Werthen von $p+p'i$ sind diejenigen auszulesen, für welche

$$\frac{4+5i-(p+p'i)^2}{-2+5i}=\frac{17+2(p^2-p'^2)-10pp'}{29}$$
$$+\frac{-30+5(p^2-p'^2)+4pp'}{29}i$$

eine ganze Zahl wird. Es findet sich darunter nur der brauchbare Werth $p+p'i=1+3i$, welcher auch noch mit entgegengesetztem Zeichen genommen werden kann, und die ganze Zahl $=-1-2i$ liefert. Nimmt man $p+p'i=1+3i$; so ist

$$K'=\frac{\sqrt{4+5i}+1+3i}{-2+5i}$$

zu entwickeln. Dies gibt

n	$P_n+P'_n i$	$Q_n+Q'_n i$	$a_n+a'_n i$
-1		$-1-2i$	
0	$1+3i$	$-2+5i$	$-i$
1	$4-i$	$3+i$	$2-i$
2	3	$-1+2i$	$-1-2i$
3	2	$2-i$	$1+i$
4	$1+i$	$1+2i$	$1-i$

etc.

Die Periode von K' stimmt vom Zeiger 4 an mit der Periode von K vom Zeiger 0 an überein. Man kann also, da die Periode achtgliederig ist, die Kombinationen

$K(0)$, (8), (16) ... *komb.* $K'(4)$
$K(0)$ *komb.* $K'(4)$, (12), (20) ...

bilden.

Für die erste Kombination der ersten Reihe $K(0)$ *komb.* $K'(4)$ hat man

n	$a_n+a'_n i$	$M_n+M'_n i$	$N_n+N'_n i$
-2		0	1
-1		1	0
0	0	0	1
1	$-1-i$	1	$-1-i$
2	$1+2i$	$1+2i$	$2-3i$
3	$-2+i$	$-3-3i$	$-2+7i$

Für die zweite Kombination der ersten Reihe $K(8)$ *komb.* $K'(4)$ hat man, mit Bezug auf die Entwickelung von K in §. 200, VI.,

n	$a_n + a_n' i$	$M_n + M_n' i$	$N_n + N_n' i$
6		$-110+50i$	$-65+8i$
7		$-173-120i$	$-70-90i$
8	0	$-110+50i$	$-65+8i$
9	$-1-i$	$-13-60i$	$3-33i$
10	$1+2i$	$-3-36i$	$4-19i$
11	$-2+i$	$29+9i$	$14+9i$

Bezeichnet man die beiden hierdurch gefundenen Auflösungen mit

$$\overset{0}{M} = -3-3i, \qquad \overset{0}{N} = -2+7i$$

$$\overset{1}{M} = 29+9i, \qquad \overset{1}{N} = 14+9i$$

so kann man alle übrigen in den obigen beiden Kombinationsreihen enthaltenen Auflösungen mittelst der aus §. 82 und 84 zu entlehnenden Rekursionsformel berechnen, für deren Anwendung der fünfte Abschnitt mehrfache Beispiele enthält.

Um eine neue Reihe von Auflösungen zu finden, hat man den zweiten Werth von K', welcher $= \frac{\sqrt{4+5i}-1-3i}{-2+5i}$ ist, zu entwickeln und wie den vorstehenden zu behandeln.

Alle hierdurch gefundenen Auflösungen sind vollkommen relativ prim. Um die etwa vorhandenen Auflösungen mit gemeinschaftlichem Maasse zu bestimmen, hat man die quadratischen Faktoren von $k = -2+5i$ zu ermitteln. Da diese Zahl eine vollkommene Primzahl ist; so kommt nur ihre Zerlegung in der Form

$$k = -ki^2 = (2-5i)i^2$$

in Betracht. Demnach suche man die Auflösungen der Gleichung

$$(1+2i)x^2 - 2(1+i)xy - (2-i)y^2 = 2-5i$$

und multiplizire jede sich ergebende mit i.

Alle durch das bisherige Verfahren gefundenen Auflösungen ohne Ausnahme können nun auch noch mit entgegengesetztem Zeichen genommen werden.

§. 204. *Beispiel mit nicht quadratischer Determinante:*

$$2x^2 + 4xy - 3y^2 = -7$$

In diesem Beispiele sind alle Koeffizienten reell. Dasselbe wird behuf allgemeiner Auflösung genau nach der generellen Regel behandelt. Es darf aber nicht übersehen werden, dass alle Kettenbrüche, gleichviel, ob imaginäre Zahlen darin vor-

kommen oder nicht, stets nach dem Prinzipe der **numerisch kleinsten Reste** zu entwickeln sind. Demnach hat man zuvörderst für $K = \frac{\sqrt{10} - 2}{2}$

n	P_n	Q_n	a_n	M_n	N_n
—2				0	1
—1		3		1	0
0	—2	2	1	1	1
1	4	—3	—2	—1	—2
2	2	—2	—3	4	7
3	4	3	2	7	12
4	2	2	3	25	43
5	4	—3	—2	—43	—74

Jetzt sind die durch 7 theilbaren Zahlen I von der Form $10 - (p + p'i)^2$ zu suchen. Nach der Regel des §. 202, IV. hat man hier, wo $q + q'i = 7$, also $q = 7$, $q' = 0$ ist, statt der dortigen Ausdrücke (6) und (7), indem der Ausdruck (5) unbeachtet bleibt,

$$(6) \quad p$$
$$(7) \quad p + (7 - p)i$$

Hierin ist p von 0 bis 7 zu variiren. Man hat also

	aus (6)	aus (7)	also in ganzen Zahlen
p	p'	p'	$p' =$
0	0	7	0, 1, 2, 3, 4, 5, 6, 7
1	0	6	0, 1, 2, 3, 4, 5, 6
2	0	5	0, 1, 2, 3, 4, 5
3	0	4	0, 1, 2, 3, 4
4	0	3	0, 1, 2, 3
5	0	2	0, 1, 2
6	0	1	0, 1
7	0	0	0

Hiervon sind diejenigen Werthe auszuwählen, wodurch

$$\frac{10 - (p + p'i)^2}{7} = \frac{10 - p^2 + p'^2}{7} - \frac{2pp'}{7} i$$

eine ganze Zahl wird. Dies ereignet sich nur für $p + p'i = 2i$ und $= 5i$. Da diese beiden Werthe in der Kathete OB des Dreiecks OAB liegen; so braucht man demnächst keine konjugirten Gruppen zu betrachten, indem die aus den vorstehenden beiden Werthen hervorgehenden einander konjugirt sind. Für den ersten Werth gibt $K' = \frac{\sqrt{10} + 2i}{7}$ die Entwickelung

n	$P_n + P_n' i$	$Q_n + Q_n' i$	$a_n + a_n' i$
—1		—2	
0	$2i$	—7	0
1	—$2i$	—2	—2+i
2	4	3	2
3	2	2	3
4	4	—3	—2

Diese Entwickelung von K' hat dieselbe Periode wie die von K. Es lassen sich also die Kombinationen

$$K(1), (5), (9) \ldots \textit{komb.}\ K'(4)$$
$$K(1)\ \textit{komb.}\ K'(4), (8), (12) \ldots$$

bilden. Da jedoch in denselben die Zeigersumme für zwei übereinstimmende Glieder unpaar ist; so liefern die hierdurch entstehenden Werthe von x und y die rechte Seite der gegebenen Gleichung mit entgegengesetztem Zeichen. Dieselben sind also sämmtlich mit i zu multipliziren.

Die ersten beiden Kombinationen der ersten Reihe ergeben

$K(1)$ *komb.* $K'(4)$				$K(5)$ *komb.* $K'(4)$			
n	$a_n + a_n' i$	$M_n + M_n' i$	$N_n + N_n' i$	n	$a_n + a_n' i$	$M_n + M_n' i$	$N_n + N_n' i$
-2		0	1				
-1		1	0	3		7	12
0	1	1	1	4		25	43
1	0	1	0	5	0	7	12
2	-3	-2	1	6	-3	4	7
3	-2	5	-2	7	-2	-1	-2
4	2—i	8—5i	-3+2i	8	2—i	2+i	3+2i

Multiplizirt man die hierdurch gefundenen Werthe mit i; so ergeben sich die beiden Auflösungen

$$\overset{0}{M} = 5 + 8i, \qquad \overset{0}{N} = -2 - 3i$$
$$\overset{1}{M} = -1 + 2i, \qquad \overset{1}{N} = -2 + 3i$$

auf welche man zur Berechnung der obigen unendlichen Menge von Kombinationen die bekannte Rekursionsformel in Anwendung bringen kann.

Dies, sowie die Berechnung der übrigen Reihen überlassen wir dem Lehrer.

§. 205. *Fall, wo die Determinante ein Quadrat ist.*

I. Wenn man auch auf den Fall, wo die Determinante ein Quadrat d^2 ist, die bisher befolgte allgemeine Auflösungsmethode in Anwendung bringen will, muss man dafür sorgen, dass die Kettenbruchsentwickelungen stets in absolut klein-

sten Zahlen schliessen, d. h. so, dass wenn die drei Grössen $P_n = d$, $Q_n = 0$ und Q_{n-1} den Schluss bilden, der absolute Werth von Q_{n-1} so klein als möglich sei. Da man ferner nach §. 88 leicht einen Zeichenwechsel in der zum Schlusse gehörigen Grösse Q_{n-1} bewirken kann; so lässt sich stets erreichen, dass der reelle Theil dieses Werthes von Q_{n-1} positiv wird, oder dass der imaginäre Theil positiv wird, insofern der reelle zufällig $= 0$ sein sollte. Einen solchen Schluss wollen wir den Schluss in kleinsten positiven Zahlen nennen. Wir setzen voraus, dass derselbe bei jeder Entwickelung erzielt werde, was nach §. 90 geschehen kann. Ist nämlich Q_{n-1} der zu untersuchende und eventuell zu reduzirende Werth irgend eines bereits erreichten Schlusses; so dividirt man mit $2d$ in Q_{n-1} nach dem Prinzipe der absolut kleinsten Reste. Der sich ergebende absolut kleinste Rest ist bekanntlich absolut $\leqq \frac{2d}{\sqrt{2}}$ d. i. $\leqq \sqrt{2}\, d$. Bezeichnen wir nun mit R eine Grösse, deren reeller Theil entschieden positiv ist, oder deren imaginärer Theil es für den Fall ist, dass der positive $= 0$ sein sollte; so stellt sich der erwähnte Rest der Division entweder als R oder als $-R$ dar. Im ersteren Falle bedient man sich der Formeln (1) und (3), im zweiten Falle dagegen der Formeln (2) und (4) aus §. 90, um zu bewirken, dass für den neuen Schluss das vorletzte Q genau $= R$ werde.

Wenn die Determinante $= 0$ ist, zerfällt auch hier die gegebene Gleichung in zwei unbestimmte Gleichungen vom ersten Grade.

II. Übrigens kann man die Auflösung der Gleichungen mit quadratischer Determinante auch nach der besonderen Regel des §. 121 bewirken, welche in mancher Beziehung als einfacher gelten kann, insofern man die Faktoren der zu zerlegenden Zahlen kennt.

Als Beispiel für das Verfahren nach §. 121 diene die Gleichung

$$2x^2 + (2 - 3i)xy - 3iy^2 = -4 + 3i$$

Da der Koeffizient von xy keine paare, vielmehr eine unvollkommen paare Zahl ist; so hat man mit 2 zu multipliziren und die Gleichung

$$4x^2 - 2(-2 + 3i)xy - 6iy^2 = -8 + 6i$$

zu behandeln.
Hierin ist die Determinante

$$D + D'i = (-2 + 3i)^2 + 4 \cdot 6i = -5 + 12i$$

Dass diese Grösse das Quadrat von $2 + 3i$ ist, erkennt man, indem man die Formel

$$\sqrt{-5+12i}=\sqrt{\frac{1}{2}(\sqrt{169}-5)}+\sqrt{\frac{1}{2}(\sqrt{169}+5)}\,.\,i=2+3i$$

in Anwendung bringt.

Nach §. 114 müssen nun

$$y=\frac{p-q}{2(2+3i)},\qquad x=\frac{p+q-2(2-3i)y}{8}$$

ganze Zahlen sein, indem p und q je zwei Faktoren darstellen, in welche sich die Grösse $4(-8+6i)=-8(4-3i)$ zerlegen lässt. Alle möglichen Werthe von p und q finden sich, wenn man die vollkommenen Primfaktoren von 8 und $4-3i$ kennt. Nun ist

$$8=i(1+i)^6$$
$$4+3i=i^3(1+2i)^2=(0+i)^3(1+2i)^2$$

also nach §. 193, IV.

$$4-3i=(0-i)^3(1-2i)^2=i(1-2i)^2$$

mithin

$$-8(4-3i)=(1+i)^6(1-2i)^2=i^4(1+i)^6(1-2i)=pq$$

Der Faktor $i^4=1$ ist dieser Zahl deshalb nochmals beigefügt, um auf den daraus hervorgehenden zulässigen Zeichenwechsel von p und q aufmerksam zu machen.

Nimmt man unter Anderem $p=i(1+i)^4(1-2i)^2=-4(4-3i)$ $q=i^3(1+i)^2=2$; so ergibt sich die Auflösung $x=-4$, $y=3i$.

III. Wir bemerken noch, dass in Ermangelung einer Faktorentafel, und wenn man nicht das praktische Verfahren aus §. 195 vorzieht, die Zerlegung einer Zahl in ihre Faktoren ein Problem ist, welches auf die Lösung einer diophantischen Gleichung vom zweiten Grade mit quadratischer Determinante zurückkommt. Die in §. 120 erläuterten Regeln, namentlich diejenigen sub II. und III., sind auch hier mit geringen Modifikationen anwendbar. Die Kaussler'sche Regel in §. 120, III. verweitläuftigt sich übrigens hier, wo es sich um komplexe Grössen handelt, in höherem Grade, als die Regel in demselben Paragraphen sub II.

§. 206. *Auflösung der allgemeinen Gleichungen vom zweiten Grade mit zwei und mehr Unbekannten in ganzen, resp. rationalen Zahlen.*

I. Die Auflösung der allgemeinen Gleichung vom zweiten Grade mit zwei Unbekannten in der Form

(1) $$ax^2-2bxy-cy^2+2dx+2ey=k$$

worin die Koeffizienten komplexe Zahlen sein können, ist nach den Regeln des §. 125 zu bewirken, indem man für die auf-

tretenden Willkürlichen u, v, w... willkürliche **komplexe** ganze Zahlen einführt.

Dabei ist nur zu bemerken, dass, um der einschlagenden Betrachtung des §. 86 auch für komplexe Zahlen Gültigkeit zu verschaffen, die dort erwähnten Reste die **absolut kleinsten** sein müssen.

II. Ebenso ist die **homogene** Gleichung mit **drei** Unbekannten in **ganzen** und **rationalen** Zahlen, sowie die **allgemeine** Gleichung mit **zwei** Unbekannten in **rationalen** Zahlen nach den Vorschriften der §§. 160 ff. zu lösen.

Hierbei machen wir darauf aufmerksam, wie aus §. 201 hervorgeht, dass durch die in §. 161 vorgeschriebenen Transformationen der absolute Werth der Determinante fortwährend verkleinert werden kann, und dass man, wenn sich hierdurch nicht schon früher eine quadratische Determinante > 1 einstellt, schliesslich immer entweder auf die Determinante $+1$ oder -1 geleitet werden muss, welche beide Quadrate, nämlich resp. $= (-1)^2$ oder $= i^2$ sind.

Da bei der Zulassung imaginärer Werthe -1 als ein vollkommenes Quadrat erscheint; so fällt hier die einschränkende Bedingung, dass in der Gleichung

$$ax^2 + by^2 + cz^2 = 0 \tag{2}$$

die drei Koeffizienten nicht gleiche Zeichen besitzen dürfen, ganz hinweg, und die Bedingungen der Lösbarkeit dieser Gleichung sind vollständig durch die Formeln (11) oder (12) in §. 168 dargestellt.

Auch bemerken wir noch, dass bei komplexen Zahlen, wo die Zerlegung in Faktoren, sowie die Prüfung auf die Eigenschaft eines vollständigen Quadrates bedeutend umständlicher ist, als bei reellen Zahlen, das in §. 167 bezeichnete Verfahren um so grössere Rechnenvortheile darbietet.

III. Die Auflösung der homogenen und allgemeinen Gleichungen mit beliebig vielen Unbekannten resp. in ganzen und in rationalen Zahlen kann unter den im achten Abschnitte namhaft gemachten Umständen ebenfalls nach den dortigen Regeln ausgeführt werden.

§. 207. *Die Grundformeln der Kongruenz komplexer Zahlen.*

I. Wir übertragen die in der Einleitung des §. 135 erläuterten Grundbegriffe über die Kongruenz der Zahlen jetzt auch auf den allgemeineren Fall, wo es sich um ganze **komplexe** Zahlen handelt.

Alsdann ist die Kongruenzformel

(1) $$a+a'i \equiv b+b'i \bmod p+p'i$$

der kürzere Ausdruck für die Gleichung

(2) $$(a+a'i)-(b+b'i)=(n+n'i)(p+p'i)$$

oder

(3) $$a+a'i=(n+n'i)(p+p'i)+(b+b'i)$$

Bestimmt man den Rest $b+b'i$ aus dem Bruche

(4) $$\frac{a+a'i}{p+p'i}=\frac{ap+a'p'}{p^2+p'^2}+\frac{a'p-ap'}{p^2+p'^2}i$$
$$=n+n'i+\frac{r}{p^2+p'^2}+\frac{r'}{p^2+p'^2}i$$
$$=n+n'i+\frac{b+b'i}{p+p'i}$$

nach §. 190, III. dergestalt, dass r und r' positiv und $<p^2+p'^2$ wird; so stellt $n+n'i$ den grössten Subquotienten jenes Bruches dar, und man kann, analog wie bei den reellen Zahlen, den Rest $b+b'i$ den kleinsten positiven Rest von $a+a'i$ nennen, wiewol schon in §. 190 bemerkt ist, dass in diesem Reste die beiden Zahlen b und b' keineswegs immer positiv ausfallen. Es ist übrigens immer der absolute Werth dieses Restes oder $\sqrt{b^2+b'^2}<\sqrt{2(p^2+p'^2)}$.

Bestimmt man jenen Rest so, dass r und r' negativ und $<p^2+p'^2$ wird; so stellt $n+n'i$ den kleinsten Superquotienten des fraglichen Bruches dar, und man kann den Rest $b+b'i$, wofür ebenfalls $\sqrt{b^2+b'^2}<\sqrt{2(p^2+p'^2)}$ sein wird, den kleinsten negativen Rest von $a+a'i$ nennen.

Wenn man will, kann man offenbar von r und r' auch die Eine positiv und die andere negativ, obwol absolut immer $<p^2+p'^2$ werden lassen, sodass von den beiden Zahlen n und n' die Eine einen grössten Super- und die andere einen kleinsten Subquotienten darstellt.

Bestimmt man jedoch nach §. 190, IV. den fraglichen Rest so, dass r und r' absolut $\leqq \frac{1}{2}(p^2+p'^2)$ wird; so erhält man $\sqrt{b^2+b'^2} \leqq \sqrt{\frac{1}{2}(p^2+p'^2)}$ und kann nun mit Recht den Rest $b+b'i$ den absolut kleinsten Rest von $a+a'i$ nach dem Model $p+p'i$ nennen. Man sieht, dass bei komplexen Zahlen der absolut kleinste Rest nicht nothwendig entweder der kleinste positive oder der kleinste negative Rest zu sein braucht, wie es bei reellen Zahlen der Fall war, wol aber ist es immer Einer der vier im Vorstehenden bezeichneten kleinsten Reste.

Zwischen den ganzen Zahlen $r+r'i$ und $b+b'i$ besteht immer die Beziehung

$$(5)\qquad b+b'i=\frac{r+r'i}{p-p'i}$$

II. Es leuchtet ein, dass alle in §. 135 sub I. bis XI. und sub XIII. bis XV. vorgetragenen Lehrsätze auch für komplexe Zahlen Gültigkeit haben, insofern man unter den primen und relativ primen Zahlen stets die vollkommen primen und vollkommen relativ primen Zahlen versteht.

Der dortige Satz XVI. erfordert jedoch bei seiner Übertragung auf komplexe Zahlen, dass man, wenn a, b, p jetzt komplexe Zahlen (n und α jedoch, wie dort, positive reelle Zahlen) bedeuten, in den Exponenten von a und b anstatt des Models p dessen Norm (also wenn der Model $=p+p'i$ gesetzt wird, den Werth $p^2+p'^2$) substituire.

Ebenso erfordert der dortige Satz XVII., dass man in den Exponenten von A und B anstatt des grössten gemeinschaftlichen Maasses m von P und Q, die Norm dieses Maasses (also wenn jenes Maass $=m+m'i$ gesetzt wird, den Werth $m^2+m'^2$) substituire.

In derselben Weise hat man in dem dortigen Satze XVIII. in den Exponenten statt des Models p dessen Norm zu substituiren.

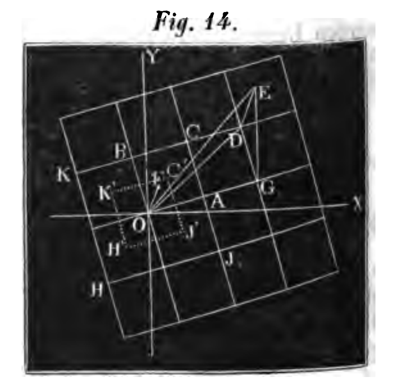
III. Der in §. 135, XII. entwickelte Satz über die Gränzen, innerhalb welcher nothwendig Eine, und auch nur Eine zu $a+a'i$ nach dem Model $p+p'i$ kongruente Zahl $b+b'i$ liegen muss, bedarf jedoch hier für komplexe Zahlen einer Erweiterung.

Das fragliche Gesetz lässt sich durch die Prinzipien des Situationskalkuls sehr anschaulich machen. Zu diesem Ende sei in Figur 14 resp. OX und OY die positiv reelle und positiv imaginäre Axe,

$$(6)\qquad (OA)=p+p'i$$

und über (OA) als Quadratseite ein Netz von Quadraten entworfen. Die vom Nullpunkte O nach den verschiedenen Netzpunkten gezogenen Linien, wie (OD), stellen dann die verschiedenen komplexen Vielfachen von (OA) dar; man hat also

Fig. 14.



$$(7)\qquad (OD)=(n+n'i)(p+p'i)$$

In unserer Figur würde man für die spezielle Lage des Punktes D

$(OD)=(OG)+(GD)=2(p+p'i)+i(p+p'i)=(2+i)(p+p'i)$

haben.

Jede beliebige Zahl $a+a'i$, welche durch (OE) vertreten sei, kann nun in zwei Theilen (OD) und (DE) dargestellt werden, von denen der erste in irgend einem Netzpunkte D endigt, also $=(n+n'i)(p+p'i)$ ist. Der zweite Theil (DE) muss dann offenbar ein zu $a+a'i$ kongruenter Rest $b+b'i$ sein. Statt der Gleichung

$$(OE)=(OD)+(DE)$$

hat man also die Gleichung

(8) $$a+a'i=(n+n'i)(p+p'i)+b+b'i$$

oder die Kongruenz

(9) $$a+a'i\equiv b+b'i \bmod p+p'i$$

Zieht man allgemein nach irgend einem Punkte E von zwei Netzpunkten, z. B. von D und G, die Geraden $(DE)=b+b'i$, $(GE)=c+c'i$; so sind dieselben in Beziehung zu der Quadratseite $(OA)=p+p'i$ als Model einander kongruent.

Denn man hat nun $(OE)\equiv(DE)$ und $(OE)\equiv(GE)$, mithin auch $(DE)\equiv(GE) \bmod (OA)$ oder $b+b'i\equiv c+c'i \bmod p+p'i$.

Ziehen wir nun von dem Endpunkte E jeder gegebenen Zahl $(OE)=a+a'i$ behuf Bestimmung eines kleinsten kongruenten Restes $b+b'i$ die Linie ED immer nach Ein und demselben, z. B. immer nach dem unteren Eckpunkte D des Quadrates, in welchem E liegt; so leuchtet ein, dass jeder Rest (DE), wenn er parallel zu sich selbst an den Nullpunkt nach (OF) getragen wird, eine von O auslaufende und in dem Quadrate $OACB$ liegende Linie sein wird.

Die in einem solchen Quadrate liegenden ganzen Zahlen (OF) sind es also, unter welchen nothwendig für jede gegebene ganze Zahl $a+a'i$ ein zum Model $p+p'i$ kongruenter Rest vorkommen wird.

Wenn das Quadrat $OACB$ so verzeichnet worden, dass $(OA)=p+p'i$ und $(OB)=i(p+p'i)$, dass also (OB) aus (OA) durch die positive Drehung von rechts nach links um 90° entstanden ist; so folgt aus der Beziehung (5) leicht, dass die darin liegenden ganzen Zahlen $b+b'i$ die kleinsten positiven Reste von $a+a'i$ sind.

In dem diametral gegenüber liegenden Quadrate OH liegen die kleinsten negativen Reste. In dem Quadrate OI wür-

den diejenigen kleinsten Reste liegen, für welche r positiv und r' negativ ist, und in dem Quadrate OK diejenigen, für welche r negativ und r' positiv ist.

Man erkennt ohne Schwierigkeit, dass von den vier eben genannten Resten, welche in dem grösseren Quadrate $HICK$ liegen, der absolut kleinste in die Gränzen des Quadrates $H'I'C'K'$ fällt, dessen Seite $H'I' = OA$, dessen Mittelpunkt aber der Nullpunkt ist. Das letztere Quadrat bezeichnet also die Gränze für die absolut kleinsten Reste.

Dass im Innern eines jeden der vorstehend betrachteten fünf Quadrate immer nur eine einzige Zahl $b+b'i$ liegen kann, welche $\equiv a+a'i$ ist, oder dass von allen diesen Zahlen keine zwei nach dem Model $p+p'i$ einander kongruent sind, leuchtet ein. Nur wenn ein solcher Rest in einer Seitenlinie eines solchen Quadrates endigt, fällt auch in die gegenüberstehende Seite ein kongruenter Rest, und wenn der erstere in einer Ecke des Quadrates endigt, fallen in die anderen drei Eckpunkte ebenfalls kongruente Reste. Von den in den Umfang eines solchen Quadrates etwa treffenden ganzen Zahlen sind also nur diejenigen zu betrachten, welche in zwei zusammenstossenden Seiten, wie OA und OB liegen, mit Ausnahme der beiden in den Eckpunkten A und B selbst endigenden.

IV. Bestimmen wir jetzt die Anzahl α der in einem Quadrate wie $OACB$ liegenden einander nicht kongruenten Zahlen, indem wir die vier Eckpunkte O, A, C, B für einen einzigen zählen und von den sonst in den Seitenlinien liegenden Zahlen nur die in OA und OB fallenden in Betracht ziehen.

Zu diesem Ende sei in Fig. 15 um die Ecken des Quadrates $OACB$ ein anderes Quadrat $PQRS$ beschrieben, dessen Seiten $= p+p'$ sind und in den Richtungen der Grundaxen liegen. Ermitteln wir nun die Anzahl der im Quadrate $PQRS$, sowie der in den Dreiecken OPA, AQC, CRB, BSO liegenden ganzen Zahlen; so ist die Differenz zwischen beiden die Anzahl α der im Quadrate $OACB$ liegenden ganzen Zahlen.

Fig. 15

Mit Ausschluss aller im Umfange liegenden ganzen Zahlen enthält das Quadrat $PQRS$ in seinem Innern offenbar deren

(10) $$\alpha_1 = (p+p'-1)(p+p'-1)$$

Was die in dem Dreiecke OPA liegenden ganzen Zahlen betrifft; so nehmen wir zuvörderst an, p und p' besitzen kein gemeinschaftliches reelles Maass > 1. Alsdann kann in der Hypotenuse OA, ausser in den Endpunkten O und A, keine ganze Zahl liegen. Die übrigen in jenem Dreiecke vorkommenden ganzen Zahlen, mit Ausschluss der in den Katheten OP, PA liegenden, sind, wenn allgemein g_n die in dem Bruche $\frac{np'}{p}$ enthaltenen grössten Ganzen bezeichnet, durch folgende Werthe von $b + b'i$ dargestellt.

b	b'
1	$1, 2, 3 \ldots g_1$
2	$1, 2, 3 \ldots g_2$
3	$1, 2, 3 \ldots g_3$
4	$1, 2, 3 \ldots g_4$
$\vdots$	
$p-1$	$1, 2, 3 \ldots g_{p-1}$

Die Anzahl dieser Werthe ist

(11) $$\alpha_2 = g_1 + g_2 + g_3 + \ldots + g_{p-1}$$

Dividirt man die sukzessiven Vielfachen von p' durch p; so hat man

$$p' = g_1 p + r_1$$
$$2p' = g_2 p + r_2$$
$$3p' = g_3 p + r_3$$
$$\vdots$$
$$(p-1)p' = g_{p-1} p + r_{p-1}$$

Da p und p' relativ prim sind; so hat man nach §. 136, VII. für die Summen der Quotienten g, indem jetzt die Reste r_1, $r_2 \ldots r_{p-1}$ alle ganzen Zahlen $1, 2, \ldots (p-1)$ enthalten,

(12) $$\alpha_2 = \frac{(p-1)(p'-1)}{2}$$

Eben so viel ganze Zahlen liegen offenbar in jedem der vier kongruenten Dreiecke OPA, AQC, CRB, BSO. Man hat also, wenn man die dem Nullpunkte O angehörige Zahl mitberücksichtigt,

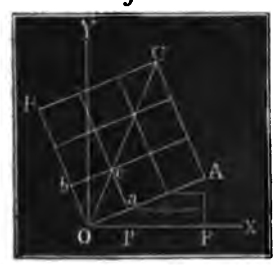
$$\alpha = \alpha_1 - 4\alpha_2 + 1 = (p+p'-1)(p+p'-1) - 2(p-1)(p'-1) + 1 \text{ d. i.}$$

(13) $$\alpha = p^2 + p'^2$$

Dieselbe Formel gilt auch für den Fall, wo p und p' das grösste gemeinschaftliche Maass $m > 1$ besitzen. Alsdann liegen

in jeder Seite des Quadrates $OACB$, wie Figur 16 zeigt, ausser in den Eckpunkten, $m-1$ ganze Zahlen.

Fig. 16.



Nimmt man nun $Oa = \frac{1}{m}\overline{OA}$ oder $(Oa) = \frac{p}{m} + \frac{p'}{m}i$, worin nun $\overline{Op} = \frac{p}{m}$ und $\overline{pa} = \frac{p'}{m}$ relativ prim sind; so liegen in dem Quadrate $Oacb$, mit Ausschluss der Ecken, nach Gl. (13) $\left(\frac{p}{m}\right)^2 + \left(\frac{p'}{m}\right)^2 - 1$ ganze Zahlen; mithin in allen m^2 kleinen Quadraten, welche das grosse Quadrat $OACB$ ausmachen, $m^2\left[\left(\frac{p}{m}\right)^2 + \left(\frac{p'}{m}\right)^2 - 1\right] = p^2 + p'^2 - m^2$. Hierzu kommen noch die in den Ecken der kleinen Quadrate liegenden Punkte, mit Ausschluss der in AC und BC liegenden. Die Anzahl dieser Punkte ist $m.m = m^2$. Demnach hat man auch hier

$$\alpha = p^2 + p'^2 - m^2 + m^2 = p^2 + p'^2$$

Dasselbe Resultat würde sich ergeben, wenn man gleich bei der Summirung der Quotienten g_1, g_2... die allgemeinere Formel (5) aus §. 136, VII. zu Grunde gelegt hätte.

Da $\sqrt{p^2 + p'^2}$ der absolute Werth des Models ist; so sind wir auf den interessanten Satz gestossen, d a s s d i e A n z a h l d e r i n e i n e m Q u a d r a t e d e r o b e n b e s c h r i e b e n e n A r t v o n d e r S e i t e n l i n i e $\sqrt{p^2 + p'^2}$ l i e g e n d e n g a n z e n Z a h l e n, u n t e r w e l c h e n s i c h n o t h w e n d i g e i n e, a b e r a u c h n u r E i n e z u $a + a'i$ n a c h d e m M o d e l $p + p'i$ k o n g r u e n t e Z a h l $b + b'i$ b e f i n d e t, g l e i c h d e m Q u a d r a t e $p^2 + p'^2$ d e s a b s o l u t e n W e r t h e s d e s M o d e l s i s t.

V. Um die vorstehenden $p^2 + p'^2$ Zahlen selbst darzustellen, kann man die Untersuchung aus §. 202, IV. zu Hülfe nehmen. Man beachte nämlich, dass wenn die Diagonale AB gezogen wird, und $b + b'i$ irgend eine Zahl im Dreiecke OAB ist, $(1+i)(p+p'i) - (b+b'i)$ eine Zahl im Dreiecke CAB ist. In dem Einen dieser beiden Dreiecke liegen also so viel ganze Zahlen, als im anderen, und nachdem man z. B. die in OAB liegenden gefunden und mit $b + b'i$ bezeichnet hat, ergeben sich die in CAB liegenden durch die Formel

(14) $(1+i)(p+p'i) - (b+b'i) = (p - p' - b) + (p + p' - b')i$

Man hat hierbei nur zu berücksichtigen, dass wenn die Zahl $b + b'i$ in die Diagonale AB selbst fällt, auch die ent-

sprechende Zahl (14) in diese Diagonale, jedoch auf die entgegengesetzte Seite des Mittelpunktes in einen gleichen Abstand von diesem fallen wird. Von diesen in der Diagonale AB paarweise vorkommenden Zahlen ist nur die Eine Hälfte zu notiren, indem sich die andere Hälfte nach der Formel (14) als dem Dreiecke CAB angehörig ergeben wird.

Nur wenn im Mittelpunkte des Quadrates $OACB$ eine ganze Zahl liegt, also Eines der eben genannten Paare von Punkten in dem Mittelpunkte der Diagonale AB zusammenfallen, ist dieser Punkt nur ein einziges Mal zu notiren. Dieser Fall charakterisirt sich übrigens sofort dadurch, dass die Formel (14) nochmals denselben Werth $b+b'i$ ergibt. Derselbe verlangt offenbar, dass $(OC)=(1+i)(p+p'i)=p-p'+(p+p')i$ durch 2 theilbar, dass also sowol $p-p'$, wie auch $p+p'$ paar sei. Dies ereignet sich immer, aber auch nur dann, wenn entweder p und p' paar oder wenn beide unpaar sind, wenn also der Model $p+p'$ entweder vollkommen paar oder vollkommen unpaar, d. h. allgemein, wenn er durch $1+i$ theilbar ist.

Ebenso wird der Werth 0 für den Nullpunkt O nur ein einziges Mal für alle vier Eckpunkte $O, A, C, B,$ und ausserdem werden die in den Katheten OA und OB liegenden Zahlen nur Ein Mal und nicht zum zweiten Male für die entsprechenden Punkte in den gegenüberliegenden Seiten notirt.

Im Übrigen sind die hiernach im Dreiecke OAB liegenden ganzen Zahlen genau dieselben, welche in §. 202, IV. zu bestimmen waren. Man hat nur nach der jetzigen Bezeichnung $p+p'i$ für $q+q'i$ und $b+b'i$ für $p+p'i$ zu nehmen, wie wenn man die durch $p+p'i$ theilbaren Zahlen I von der Form

$$I=D+D'i-(b+b'i)^2$$

aufsuchen wollte.

Demnach hat man, nachdem man dafür gesorgt hat, dass p und p' positiv sind, was immer zulässig ist,

$$\text{in (15)}\quad b-\frac{p}{p'}bi \qquad b \text{ von } -p' \text{ bis } 0$$

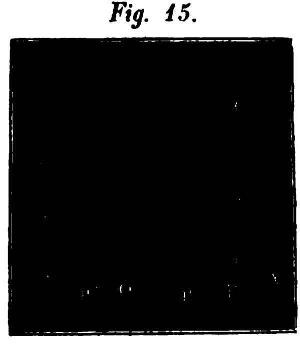
$$\text{(16)}\quad b+\frac{p'}{p}bi \qquad » \;» \;\; 0 \;» \; p$$

$$\text{(17)}\quad p+\left(\frac{p^2+p'^2}{p+p'}+\frac{p'-p}{p+p'}b\right)i \qquad » \;» \; -p' \;» \; p$$

variiren zu lassen.

VI. Man kann auch zu vorstehendem Zwecke folgendermaassen verfahren. Man notirt erst alle im Innern des Qua-

Fig. 15.



drates $PQRS$ (Fig. 15) liegenden ganzen Zahlen, mit Ausschluss der im Umfange selbst liegenden. Diese Zahlen sind durch $b+b'i$ dargestellt, wenn man darin b von $-(p'-1)$ bis $p-1$ und gleichzeitig b' von 1 bis $p-1$ variiren lässt.

Hiervon schliesst man zunächst die im Innern des Dreiecks OPA liegenden ganzen Zahlen $b+b'i$ nach der Formel (16) aus, indem man darin b von 1 bis $p-1$ wachsen lässt. Die hierdurch in der Hypotenuse OA selbst sich ergebenden Zahlen werden nicht ausgeschlossen.

Drehet man das Dreieck OPA von rechts nach links um 270° und verrückt dasselbe alsdann parallel zu $(OB)=(p+p'i)i$; so erhält man das Dreieck BSO. Demnach substituirt man ferner die soeben genannten Zahlen $b+b'i$ des Dreiecks OPA in die Formel

$$(p+p'i)i+(b+b'i)i^3=[p+p'i-(b+b'i)]i$$

und schliesst auch die hierdurch dargestellten Zahlen aus.

In ähnlicher Weise erhellet, dass wegen des Dreiecks AQC die Zahlen

$$(p+pi)+(b+b'i)i$$

und wegen des Dreiecks CRB die Zahlen

$$(p+p'i)(1+i)-(b+b'i)$$

auszuschliessen sind. In den letzten beiden Formeln hat man unter $b+b'i$ die Zahlen des Dreiecks OPA, jedoch ohne die in der Hypotenuse OA liegenden Werthe zu verstehen, weil die in AC und CB liegenden Zahlen in der That ausgeschlossen werden müssen.

Endlich ist wegen des Nullpunktes O die Zahl 0 zu notiren.

VII. Die soeben genannten ganzen Zahlen $b+b'i$ des Quadrates $OACB$ bilden die kleinsten positiven Reste aller möglichen Zahlen nach dem Model $p+p'i$. Will man die kleinsten negativen Reste haben, welche in dem Quadrate OH liegen; so hat man die vorstehenden mit -1 zu multipliziren. Die im Quadrate OK und die im Quadrate OI liegenden Reste ergeben sich dagegen durch Multiplikation der ersteren resp. mit i oder mit $-i$, indem diese Multiplikationen einer Drehung des Quadrates $OACB$ resp. um 90° oder um 270° entsprechen.

Will man endlich die **absolut kleinsten** Reste bilden, welche in dem Quadrate $H'I'C'K'$ liegen; so hat man zwei Fälle zu unterscheiden.

Erstens den Fall, wo $p+p'i$ durch $1+i$ theilbar ist, also ein Rest im Mittelpunkte des ersten oder im oberen Eckpunkte C' des zweiten Quadrates liegt. Man hat alsdann die Punkte des ersten Quadrates um $(CC') = -\frac{1}{2}(p+p'i)(1+i)$ zu verschieben. Dies gibt für die gesuchten Reste den Ausdruck $b+b'i-\frac{1}{2}(p+p'i)(1+i)$.

Zweitens den Fall, wo $p+p'i$ nicht durch $1+i$ theilbar ist, also **kein** Rest in dem gedachten Mittelpunkte, resp. Eckpunkte liegt. Man findet dann leicht, dass, jenachdem $p \gtrless p'$ ist, die Verschiebung resp. um die Entfernung $-\frac{1}{2}[(p+p'i)\times(1+i) \pm 1+i]$ geschehen müsse, wodurch sich die Werthe

$$b+b'i-\frac{1}{2}[(p+1)+p'i](1+i)$$

resp.

$$b+b'i-\frac{1}{2}[p+(p'+1)i](1+i)$$

ergeben.

§. 208. Der Fermatsche Lehrsatz für komplexe Zahlen.

I. Es sei $p+p'i$ eine vollkommene, in $a+a'i$ nicht enthaltene Primzahl von unpaarer Form (also verschieden von $1+i$ oder allgemein von $(1+i)i^n$). Ist dann $b+b'i$ der Vertreter irgend Einer der im vorigen Paragraphen bezeichneten Zahlen des Quadrates $OACB$, mit Ausschluss der im Nullpunkte liegenden Zahl 0, deren Gesammtmenge also $=p^2+p'^2-1$ ist; so bilde man die Produkte aus $a+a'i$ und allen diesen Zahlen, also die Produkte von der Form $(a+a'i)(b+b'i)$. Von diesen Produkten können keine zwei nach dem Model $p+p'i$ einander kongruent sein. Denn wäre z. B.

$$(a+a'i)(b_1+b_1'i) \equiv (a+a'i)(b_2+b_2'i)$$

so müsste, da $a+a'i$ und der Model $p+p'i$ relativ prim sind, auch $b_1+b_1'i \equiv b_2+b_2'i$ sein, was nach dem vorhergehenden Paragraphen unmöglich ist.

Bildet man daher die kleinsten positiven Reste aller jener Produkte, und bezeichnet dieselben mit $c+c'i$, sodass man

$$(a+a'i)(b+b'i) \equiv c+c'i$$

hat; so müssen unter den Resten $c+c'i$ alle Zahlen $b+b'i$ enthalten sein.

Multiplizirt man jetzt die so entstehenden $p^2+p'^2-1$ Kongruenzen miteinander, und setzt das Produkt

$$(b_1+b_1'i)(b_2+b_2'i)\ldots = (c_1+c_1'i)(c_2+c_2'i)\ldots = k$$

so erhält man

$$k(a+a'i)^{p^2+p'^2-1} \equiv k$$

Da aber jeder Faktor von k relativ prim zum Model $p+p'i$ ist; so ist es auch das Produkt k. Dividirt man also die vorstehende Kongruenz mit k; so kommt

(1) $$(a+a'i)^{p^2+p'^2-1} \equiv 1 \; mod \, p+p'i$$

In dieser Formel besteht der für komplexe Zahlen erweiterte **Fermatsche Lehrsatz**, welcher natürlich in dieser Form auch für reelle Zahlen Gültigkeit hat. Derselbe sagt aus, dass die Potenz der Zahl $a+a'i$ vom Grade $p^2+p'^2-1$, wenn man 1 davon subtrahirt, durch die vollkommene Primzahl $p+p'i$ theilbar ist.

II. Da für jede Primzahl $p+p'i$ (mit Ausnahme der Zahl $1+i$) die Norm $p^2+p'^2$ unpaar, also $p^2+p'^2-1$ paar ist; so kann man die Gl. (2) in der Form

$$[(a+a'i)^{\frac{1}{2}(p^2+p'^2-1)}+1][(a+a'i)^{\frac{1}{2}(p^2+p'^2-1)}-1]=(v+v'i)(p+p'i)$$

schreiben. Weil nun $p+p'i$ eine Primzahl ist; so muss sie in Einem der beiden Faktoren der linken Seite aufgehen. Man hat also

(2) $$(a+a'i)^{\frac{1}{2}(p^2+p'^2-1)} \equiv \pm 1 \; mod \, p+p'i$$

Für den besonderen Fall, dass $p+p'i=1+i$ ist, hat man, weil $p+p'i$ nicht in $a+a'i$ aufgehen soll, also die letztere Zahl unvollkommen paar oder unpaar sein muss, $a+a'i \equiv 1$ und auch $\equiv -1 \; mod \, 1+i$. Demnach ist jede beliebige Potenz von $a+a'i \equiv 1$ und auch $\equiv -1 \; mod \, 1+i$.

III. Da für jede Primzahl $p+p'i$ (mit Ausnahme der Zahl $1+i$) die Grösse $p^2+p'^2$ von der Form $4n+1$ ist (§. 194, II.); so ist $p^2+p'^2-1=4n$ ein Vielfaches von 4, folglich $\frac{1}{2}(p^2+p'^2-1)$ eine paare und $\frac{1}{4}(p^2+p'^2-1)$ eine ganze Zahl.

Hieraus und aus der Gleichung (2) folgt leicht, dass $(a+a'i)^{\frac{1}{4}(p^2+p'^2-1)}$ entweder $\equiv 1$ oder $\equiv -1$ oder $\equiv i$ oder $\equiv -i$ sei. Man hat also

(3) $$(a+a'i)^{\frac{1}{4}(p^2+p'^2-1)} \equiv i^m \; mod \, p+p'i$$

IV. Nimmt man in den vorstehenden Formeln (1) bis (3) statt $p+p'i$ den Model $p-p'i$; so ändere sich die Grösse $p^2+p'^2-1$ und überhaupt die linke Seite dieser Kongruenzen nicht. Da nun $p+p'i$ und $p-p'i$ zwei ganz verschiedene vollkommene Primzahlen sind, welche nicht durch Multiplikation mit Potenzen von i einander gleich werden; so gelten die obigen Kongruenzen offenbar auch dann noch, wenn man für den Model das Produkt $(p+p'i)(p-p'i)=p^2+p'^2$ nimmt. So ist unter Anderem nach (1)

(4) $$(a+a'i)^{p^2+p'^2-1} \equiv 1 \; mod \, p^2+p'^2$$

V. Was die in §. 140 für reelle Zahlen nachgewiesene Verallgemeinerung des Fermatschen Lehrsatzes für den Fall betrifft, wo der Model $P+P'i$ eine zusammengesetzte, aber zu $A+A'i$ relativ prime Zahl von der Form

(5) $$P+P'i=(p+p'i)^{\alpha}(q+q'i)^{\beta}(r+r'i)^{\gamma}\ldots$$

ist, worin $p+p'i$, $q+q'i\ldots$ vollkommene Primzahlen darstellen; so findet man durch eine ähnliche Schlussfolgerung wie dort, wenn man

(6) $$\varphi=(p^2+p'^2-1)(p^2+p'^2)^{\alpha-1}(q^2+q'^2-1)(q^2+q'^2)^{\beta-1}\ldots$$

setzt.

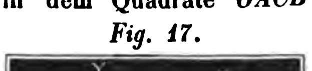
(7) $$(A+A'i)^{\varphi}\equiv 1 \mod P+P'i$$

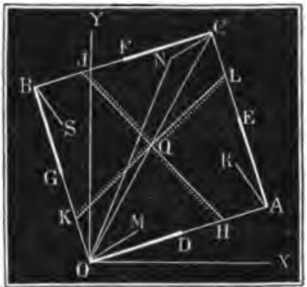
Wir bemerken noch, dass φ die Anzahl der zu $P+P'i$ relativ primen Zahlen darstellt, welche in dem Quadrate $OACB$ liegen, dessen Seite $(OA)=P+P'i$ ist. Diese Anzahl ist auch gleich der Menge der reellen Zahlen, welche relativ prim zur Norm $P^2+P'^2$ des Models und kleiner als diese Norm sind.

VI. Der letztere Satz gewährt, ähnlich wie in §. 140, II., das Mittel, die Auflösung der unbestimmten Gleichungen vom ersten Grade in allgemeinen Zeichen zu bewirken.

§. 209. *Fernerweite Beziehungen zwischen den Resten der Potenzen und der Vielfachen einer komplexen Zahl.*

I. Fassen wir nochmals die in dem Quadrate $OACB$ (Fig. 17) liegenden ganzen Zahlen ins Auge. Es sei $(OA)=p+p'i$ eine vollkommene Primzahl. Alsdann können, ausser in den vier Eckpunkten, nur in dem Falle ganze Zahlen in den Seitenlinien des Quadrates liegen, wenn $p'=0$, also $p+p'i$ eine in die Axe OX fallende reelle Zahl ist. Die vier Eckpunkte schliessen wir stets aus, sodass wir im Ganzen $p^2+p'^2-1$ ganze Zahlen zu betrachten haben. In dem eben erwähnten speziellen Falle aber, wo die vollkommene Primzahl $p+p'i$ reell (mithin von der Form $4n+3$) ist, vertheilen wir die in den Umfangslinien liegenden ganzen Zahlen so, dass wir immer nur die in den **Hälften** OD, AE, CF, BG der betreffenden Seitenlinien liegenden Zahlen nehmen und die in den anderen Hälften DA, EC, FB, GO liegenden ausschliessen (also nicht, wie früher in §. 207, alle in OA und


Fig. 17.



OB liegenden nehmen und alle in *CA* und *CB* liegenden ausschliessen). In diesem Falle beachten wir auch, dass niemals eine ganze Zahl weder in den Mittelpunkt einer Seitenlinie, noch in den Mittelpunkt des Quadrates fallen kann.

Den Fall, wo die vollkommene Primzahl $p+p'i=1+i$ ist, wo also nur eine einzige, im Mittelpunkte des Quadrates endigende ganze Zahl i in Betracht kommen würde, nehmen wir von der nachfolgenden Untersuchung aus.

In allen übrig bleibenden Fällen ist also $p^2+p'^2-1$ eine Zahl von der Form $4n$, und von diesen $4n$ Zahlen sind niemals zwei nach dem Model $p+p'i$ einander kongruent.

Ist $(OM)=b+b'i$ irgend eine dieser $p^2+p'^2-1$ ganzen Zahlen; so ist auch, wenn *CN* parallel und gleich *MO* ist, $(ON)=(OC)+(CN)=(OC)-(OM)=(p+p'i)(1+i)-(b+b'i)$ eine solche und zwar eine von (OM) verschiedene. Je zwei dieser Zahlen wie (OM) und (ON) ergänzen sich also zu der Summe $(OC)=(p+p'i)(1+i)$. Bezeichnet man demnach die Summe aller in dem Quadrate *OACB* liegenden ganzen Zahlen mit $B+B'i$; so hat man

$$(1)\quad B+B'i=\tfrac{1}{2}(p^2+p'^2-1)(p+p'i)(1+i)$$
$$=\tfrac{1}{2}(p-p')(p^2+p'^2-1)+\tfrac{1}{2}(p+p')(p^2+p'^2-1)i$$

II. Ist $a+a'i$ eine ganze Zahl, in welcher die vollkommene Primzahl $p+p'i$ nicht enthalten ist; so bilde man die Produkte aus $a+a'i$ und allen Zahlen $b+b'i$. Dies gebe, wenn $c+c'i$ die in demselben Quadrate *OACB* liegenden kleinsten Reste jener Produkte sind, eine Gruppe (G) von Gleichungen

$$(G)\quad \begin{cases}(a+a'i)(b_1+b_1'i)=(v_1+v_1'i)(p+p'i)+c_1+c_1'i\\(a+a'i)(b_2+b_2'i)=(v_2+v_2'i)(p+p'i)+c_2+c_2'i\\ \quad\text{etc.}\qquad\qquad\qquad\qquad \text{etc.}\end{cases}$$

Die Anzahl dieser Gleichungen ist $p^2+p'^2-1$ und unter den Resten $c+c'i$ kommen alle Zahlen $b+b'i$ vor. Addirt man also alle diese Gleichungen; so ergibt sich, wenn man die Summe der Quotienten $v+v'i$ mit $V+V'i$ bezeichnet,

$$(a+a'i)(B+B'i)=(V+V'i)(p+p'i)+B+B'i$$

also wegen Gl. (1)

$$(2)\quad V+V'i=\tfrac{1}{2}(p^2+p'^2-1)(a-1+a'i)(1+i)$$
$$=\tfrac{1}{2}(a-a'-1)(p^2+p'^2-1)+\tfrac{1}{2}(a+a'-1)(p^2+p'^2-1)i$$

III. Zieht man durch den Mittelpunkt Q des Quadrates *OACB* eine gerade Linie *HI*; so wird dadurch dieses Quadrat in zwei kongruente Hälften zerlegt. Insofern in der Halbirungslinie *HI* ganze Zahlen endigen, rechnen wir die in *QH* liegenden zur vorderen Hälfte *OHIB* und die in *QI* liegenden zur

hinteren Hälfte $CIHA$ (was in der Figur durch die Punktirung der vorderen und hinteren Seite resp. von QH und QI angedeutet ist). Alsdann lässt sich behaupten, dass in jede Hälfte des Quadrates die Hälfte, also $\frac{1}{2}(p^2+p'^2-1)$ der im ganzen Quadrate liegenden ganzen Zahlen anzutreffen sind. Dies leuchtet ein, wenn man erwägt, dass für die in der ersten Hälfte liegende Zahl $(OM)=b+b'i$ die Zahl (ON) $=(p+p'i)(1+i)-(b+b'i)$ in der entgegengesetzten Hälfte liegt.

Stellt man aus der Gruppe (G) der $p^2+p'^2-1$ Gleichungen diejenige Hälfte zusammen, für welche die Faktoren $b+b'i$ die in der Einen Quadrathälfte $OHIB$ liegenden Zahlen sind; so werden von den Resten $c+c'i$ eine gewisse Menge in derselben Hälfte, die übrigen aber, deren Menge $=m$ sei, in der entgegengesetzten Hälfte $CIHA$ liegen. Schreibt man für jeden der letzteren s Reste wie (ON) den Werth $(OC)-(OM)$; so muss (OM) ein in der ersten Quadrathälfte liegende Zahl sein. Diese Zahl (OM) ist aber auch verschieden von dem zuerst genannten in derselben Hälfte liegenden Reste; denn wäre sie einem solchen Reste gleich; so würde man zwei Gleichungen von der Form

$$(a+a'i)(b_1+b_1'i)=(v_1+v_1'i)(p+p'i)+(OM)$$
$$(a+a'i)(b_2+b_2'i)=(v_2+v_2'i)(p+p'i)+(OC)-(OM)$$

haben, und aus der Addition dieser Gleichungen würde folgen, weil $(OC)=(1+i)(p+p'i)$ also ein Vielfaches von $p+p'i$ ist, dass die Summe der beiden in derselben Hälfte liegenden Zahlen $b_1+b_1'i$ und $b_2+b_2'i$ durch $p+p'i$ theilbar sei, was unmöglich ist, da diese Summe weder $=(OA)$, noch $=(OB)$, noch $=(OC)$ werden kann.

Nimmt man nun nach der eben erwähnten Substitution statt der bezeichneten $\frac{1}{2}(p^2+p'^2-1)$ Gleichungen der Gruppe (G) die gleichbedeutenden Kongruenzen von der Form

$$(a+a'i)(b+b'i)\equiv c+c'i$$

so werden auf der rechten Seite unter den Grössen $c+c'i$ die Zahlen $b+b'i$ der ersten Quadrathälfte vorkommen, indem jedoch deren m mit -1 multiplizirt erscheinen. Bildet man das Produkt aller dieser Kongruenzen, und beachtet, dass die daraus entstehende Kongruenz durch das Produkt der Grössen $b+b'i$ dividirt werden kann; so ergibt sich

$$(3) \qquad (a+a'i)^{\frac{1}{2}(p^2+p'^2-1)}\equiv(-1)^m \bmod p+p'i$$

Hierdurch findet die Formel (3) im vorhergehenden Paragraphen eine nähere Erläuterung.

IV. Zieht man durch den Mittelpunkt Q des Quadrates eine auf HI perpendikular stehende Linie KL; so wird dadurch

das Quadrat in vier kongruente Viertel zerlegt. Bezeichnen wir das 1ste, 2te, 3te, 4te Viertel durch die Eckpunkte O, A, C, B; so sollen die in QH, QL, QI, QK liegenden ganzen Zahlen resp. zum 1sten, 2ten, 3ten, 4ten Viertel gehören (was in der Figur durch Punktirung angedeutet ist).

Man kann alsdann behaupten, dass von allen im ganzen Quadrate zu betrachtenden Zahlen in jedem Viertel der vierte Theil, also $\frac{1}{4}(p^2+p'^2-1)$ liegen. Denn wird AR perpendikular und gleich OM genommen, und $(OM)=b+b'i$ gesetzt; so hat man $(AR)=(b+b'i)i$ und $(OR)=(OA)+(AR)=p+p'i+(b+b'i)i$, und wenn (OM) im ersten Viertel liegt, liegt (OR) im zweiten.

In ähnlicher Weise hat man $(CN)=-(b+b'i)$ und $(ON)=(p+p'i)(1+i)-(b+b'i)$, und wenn $(OM)=b+b'i$ im ersten Viertel liegt, liegt (ON) im dritten.

Endlich hat man $(BS)=-(b+b'i)i$ und $(OS)=(p+p'i)i-(b+b'i)i$ und wenn $(OM)=b+b'i$ im ersten Viertel liegt, liegt (OS) im vierten.

Stellt man aus der obigen Gruppe (G) von Gleichungen diejenigen $\frac{1}{4}(p^2+p'^2-1)$ zusammen, für welche die Faktoren $b+b'i$ im ersten Quadratviertel liegen; so werden darunter resp. r, s, t, u sein, deren Reste $c+c'i$ im ersten, zweiten, dritten, vierten Viertel liegen. Für jeden der im zweiten Viertel liegenden s Reste substituire man die Form

$$p+p'i+(c+c'i)i$$

für jeden der im dritten Viertel liegenden t Reste die Form

$$(p+p'i)(1+i)-(c+c'i)=(p+p'i)(1+i)+(c+c'i)i^2$$

und für jeden der im vierten Viertel liegenden u Reste die Form

$$(p+p'i)i-(c+c'i)i=(p+p'i)i+(c+c'i)i^3$$

Die hierdurch in den Resten erscheinenden Zahlen $c+c'i$ werden sämmtlich verschieden und gleich den im ersten Viertel liegenden Zahlen $b+b'i$ sein.

Nimmt man nun statt der eben erwähnten Gleichungen die gleichbedeutenden Kongruenzen, multiplizirt dieselben miteinander und dividirt die sich ergebende Kongruenz durch das Produkt der Zahlen $b+b'i$ des ersten Viertels; so ergibt sich

$$(4) \qquad (a+a'i)^{\frac{1}{4}(p^2+p'^2-1)} \equiv i^{s+2t+3u} \mod p+p'i$$

Hierdurch findet die Formel (4) im vorhergehenden Paragraphen eine nähere Erläuterung.

Wenn man die Kongruenz (4) quadrirt; so kommt

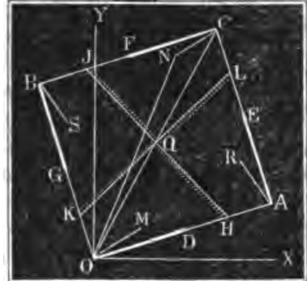
$$(5) \qquad (a+a'i)^{\frac{1}{2}(p^2+p'^2-1)} \equiv (-1)^{s+u} \mod p+p'i$$

welche in einer anderen Weise als die Kongruenz (3) die Formel (3) des vorhergehenden Paragraphen erklärt.

§. 210. **Der Wilsonsche Lehrsatz für komplexe Zahlen.**

I. Betrachten wir nochmals die im Quadrate $OACB$ (Fig. 17) liegenden ganzen Zahlen mit Ausschluss der Eckpunkte. Es sei der Model $(OA) = p + p'i$ eine vollkommene Primzahl von unpaarer Norm. Für den Fall, dass diese Primzahl reell ist, bleibt es gleichgültig, ob man die in den Umfang des Quadrates fallenden ganzen Zahlen nach §. 207 oder nach §. 209 vertheilt.

Fig. 17.



Wenn man BS parallel zur reellen Axe und $= 1$ nimmt; so ist $(OS) = (OB) + (BS) = (p + p'i)i + 1$ Eine der fraglichen im Quadrate liegenden ganzen Zahlen. Insofern $p + p'i$ reell ist, also OA in die reelle Axe fällt, liegt nicht die eben bezeichnete Zahl, wol aber die reelle Einheit 1 selbst in jenem Quadrate. Es ist also klar, dass es unter den Zahlen des Quadrates stets Eine, aber auch nur Eine gibt, welche $\equiv 1$ ist, und welche wir mit $c + c'i$ bezeichnen wollen.

Ist nun $a + a'i$ irgend eine beliebige ganze Zahl des Quadrates, also jedenfalls relativ prim zu $p + p'i$; so ist nach §. 210, I. klar, dass es irgend ein Vielfaches von $a + a'i$ geben muss, welches der Zahl $c + c'i$ kongruent ist, und zwar ein solches, dessen zweiter Faktor $b + b'i$ ebenfalls in dem Quadrate liegt und von allen diesen Zahlen der einzige ist, welcher jener Bedingung genügt. Man hat also

$$(1) \qquad (a + a'i)(b + b'i) \equiv c + c'i \equiv 1$$

Zwei solche Zahlen, wie $a + a'i$ und $b + b'i$, deren Produkt der positiven reellen Einheit nach dem Model $p + p'i$ kongruent ist, heissen Gefährten.

Wenn man AR parallel XO und $= 1$ nimmt; so ist $(OR) = p + p'i - 1$. Wäre $p + p'i$ reell; so hat man, wenn die im Umfange des Quadrates liegenden Zahlen nach §. 207 vertheilt sind, gleichfalls $(OR) = p + p'i - 1$ zu nehmen: wenn jedoch die im Umfange des Quadrates liegenden Zahlen nach §. 209 vertheilt sind; so hat man $(CN) = -1$ und statt (OR) die Zahl $(ON) = (p + p'i)(1 + i) - 1$ zu nehmen. Es gibt also unter den Zahlen des Quadrates stets Eine, aber auch nur Eine, welche $\equiv -1$ ist, und welche wir mit $d + d'i$ bezeichnen wollen.

Dass jede Zahl des Quadrates, wie $a + a'i$ einen in demselben Quadrate liegenden Gefährten $b + b'i$, und auch nur einen einzigen solchen Gefährten hat, ist nach dem Obigen klar.

Es sind aber auch je zwei Gefährten von einander verschieden, mit Ausnahme der beiden Fälle, wo ein Gefährte $\equiv 1$, also $= c + c'i$, oder wo er $\equiv -1$, also $= d + d'i$ ist.

Denn damit in der Formel (1) $a + a'i = b + b'i$ sei, muss man haben

$$(a + a'i)^2 \equiv 1 \quad \text{also}$$
$$(a + a'i)^2 - 1 = (a + a'i + 1)(a + a'i - 1) \equiv 0$$

Es muss also entweder der Faktor $a + a'i - 1$ oder der Faktor $a + a'i + 1$ durch $p + p'i$ theilbar, also entweder $a + a'i \equiv 1$, also $= c + c'i$, oder $a + a'i \equiv -1$, also $= d + d'i$ sein.

Der Gefährte von $c + c'i$ ist also ebenfalls $c + c'i$ und der von $d + d'i$ ebenfalls $d + d'i$. Von jeder anderen Zahl ist der Gefährte verschieden und niemals gleichzeitig der Gefährte einer anderen Zahl.

Gruppirt man also die im Quadrate liegenden Zahlen mit vorläufigem Ausschlusse der beiden Zahlen $c + c'i$ und $d + d'i$ so, dass immer zwei Gefährten zusammenstehen; so wird das Produkt aus diesen $p^2 + p'^2 - 3$ Zahlen $\equiv 1$ sein. Da nun $(c + c'i)(d + d'i) \equiv -1$ ist; so ist klar, dass das Produkt aller $p^2 + p'^2 - 1$ Zahlen des Quadrates $\equiv -1$ ist. Man hat also, wenn man dieses Produkt mit P bezeichnet,

$$(2) \qquad P \equiv -1 \mod p + p'i$$

Hierin besteht der für komplexe Zahlen erweiterte Wilsonsche Lehrsatz.

II. Wenn $p + p'i$ keine vollkommene Primzahl ist; so lässt sich auch $P + 1$ nicht durch $p + p'i$ theilen. Denn jeder Faktor von $p + p'i$ hat einen absoluten Werth $< \sqrt{p^2 + p'^2}$; derselbe wird also (nachdem man ihn nöthigenfalls noch mit einer Potenz von i multiplizirt hat) unter den Zahlen des Quadrates $OACB$ vorkommen, aus welchen das Produkt P besteht. Da mithin P, nicht aber 1 durch jenen Faktor theilbar ist; so kann auch $P + 1$ nicht durch denselben, folglich auch nicht durch $p + p'i$ theilbar sein.

Demnach bildet der erweiterte Wilsonsche Lehrsatz in Verbindung mit diesem Nachsatze ein Kriterium für eine vollkommene Primzahl.

Im Übrigen lässt sich der Wilsonsche Lehrsatz für den Fall, dass der Model $p + p'i$ keine vollkommene Primzahl sei, ähnlich wie in §. 145, III. dahin erweitern, dass das Produkt aus den im Quadrate $OACB$ liegenden zu $p + p'i$ relativ primen Zahlen $\equiv -1 \mod p + p'i$ sei.

III. Jede Zahl des Quadrates $OACB$, welche in einer Quadrathälfte wie $OHIB$ liegt, wobei man jedoch die etwa in den Umfang und in die Halbirungslinie des Quadrates fallen-

den Zahlen nach §. 209 und nicht nach §. 207 zu vertheilen hat, ergänzt sich mit einer in der anderen Hälfte $CIHA$ liegenden Zahl zu der Diagonale (OC), welche ein Vielfaches von $p+p'i$ ist. Wenn also die erste Zahl $\equiv a+a'i$ ist, ist die andere $\equiv -(a+a'i)$. Bezeichnet man daher das Produkt der in einer Quadrathälfte liegenden Zahlen, deren Gesammtmenge in der Voraussetzung, dass $p+p'i$ vollkommen prim sei, $\frac{1}{2}(p^2+p'^2-1)=2n$ ist, mit Q; so hat man offenbar

$$P\equiv(-1)^{\frac{1}{2}(p^2+p'^2-1)}Q^2\equiv Q^2$$

also, da nach (2) $P\equiv-1$ ist,

(3) $$Q^2\equiv-1 \mod p+p'i$$

Hieraus folgt auch $Q^2+1=(Q+i)(Q-i)=$ einem Vielfachen von $p+p'i$. Es muss also, da $p+p'i$ eine Primzahl ist, entweder $Q+i$ oder $Q-i$ durch $p+p'i$ theilbar sein. Demnach ist

(4) $$Q\equiv\mp i \mod p+p'i$$

IV. Wenn $a+a'i$ eine in dem Quadratviertel $OHQK$ liegende Zahl ist; so gibt es in dem zweiten Viertel $ALQH$ eine Zahl $p+p'i+(a+a'i)i\equiv(a+a'i)i$, ferner in dem dritten Viertel $CIQL$ eine Zahl $(p+p'i)(1+i)-(a+a'i)\equiv-(a+a'i)\equiv(a+a'i)i^2$ und in dem vierten Viertel $BKQI$ eine Zahl $(p+p'i)i-(a+a'i)i\equiv-(a+a'i)i\equiv(a+a'i)i^3$. Bezeichnet man also das Produkt der in einem Quadratviertel liegenden Zahlen, deren Gesammtmenge $\frac{1}{4}(p^2+p'^2-1)=n$ ist, mit R; so hat man offenbar

$$P\equiv i^n i^{2n} i^{3n} R^4\equiv(-1)^n R^4$$

also, da nach (2) $P\equiv-1$ ist,

(5) $$R^4\equiv(-1)^{n+1}\equiv(-1)^{\frac{1}{4}(p^2+p'^2+3)} \mod p+p'i$$

Ist also in der Zahl $p^2+p'^2=4n+1$ die Grösse n unpaar; so hat man $R^4\equiv1$. Ist dagegen n paar; so hat man $R^4\equiv-1$.

§. 211. *Kongruenzen höherer Grade. — Quadratische Reste.*

I. Im Allgemeinen haben die Sätze des §. 146 über die Kongruenzen höherer Grade auch für den Fall Gültigkeit, wo die Koeffizienten und Wurzeln der Kongruenzen komplexe Zahlen sind.

Man hat jedoch jetzt unter Primzahlen stets vollkommene Primzahlen zu verstehen. Ferner hat man zu beachten,

dass wenn $p+p'i$ der Model ist, jetzt immer $p^2+p'^2$ ganze Zahlen in einem Quadrate zusammenliegen, unter denen sich nothwendig Eine finden muss, welche irgend einer gegebenen Zahl $a+a'i$ nach jenem Model kongruent ist, aber auch nur Eine, insofern der Model vollkommen prim ist. Im letzteren Falle sind auch diejenigen $p^2+p'^2-1$ ganzen Zahlen jenes Quadrates, welche nach Ausschluss der Null übrig bleiben, relativ prim zum Model. Im Übrigen überlassen wir es dem Leser, die hieraus hervorgehenden Modifikationen der Gesetze des §. 146, deren Entwickelung keine Schwierigkeit hat, näher zu spezialisiren.

II. Die in §. 147, I. erläuterten Begriffe über quadratische Reste und Nichtreste finden auch bei komplexen Zahlen unbedingte Anwendung.

Für diese Reste ist der dem Lehrsatz des §. 147, II. analoge Satz von besonderer Wichtigkeit. Derselbe lautet hier folgendermaassen.

Wenn $p+p'i$ eine in $a+a'i$ nicht aufgehende vollkommene Primzahl von unpaarer Norm ist; so ist $a+a'i$ quadratischer Rest oder Nichtrest nach $p+p'i$, jenachdem man hat

$$(a+a'i)^{\frac{1}{2}(p^2+p'^2-1)} \equiv 1 \text{ oder } \equiv -1 \mod p+p'i$$

und im ersteren Falle gibt es in jeder Quadrathälfte wie *OHIB* einen Werth für $x+x'i$, welcher die Kongruenz

$$a+a'i \equiv (x+x'i)^2 \mod p+p'i$$

erfüllt.

Der Beweis dieses Satzes lässt sich hier ähnlich wie in §. 147 führen, wenn man den erweiterten Fermatschen Lehrsatz aus §. 208 zu Hülfe nimmt und hier immer die in dem ganzen und in dem halben Quadrate liegenden Zahlen, deren Menge resp. $p^2+p'^2-1$ und $\frac{1}{2}(p^2+p'^2-1)$ ist, betrachtet, wo dort resp. die positiven Zahlen betrachtet wurden, deren Menge resp. $p-1$ und $\frac{1}{2}(p-1)$ war.

III. Wenn sowol die Zahl $a+a'i$, als auch die vollkommene Primzahl $p+p'i$ reell ist; so hat man stets $a^{\frac{1}{2}(p^2-1)} = (a^{p-1})^{\frac{p+1}{2}} \equiv 1 \mod p$. Demnach ist jede reelle Zahl a quadratischer Rest nach jeder vollkommenen reellen Primzahl p (welche letztere immer die Form $4n+3$ besitzt).

§. 212. ***Zurückführung der komplexen Reste auf reelle.***

I. Wir gehen zunächst von der Voraussetzung aus, dass der Model $p+p'i$ eine vollkommene und auch wirklich komplexe Primzahl sei, sodass darin weder p, noch p' gleich Null ist. Ferner sei $a+a'i$ eine beliebige Zahl, in welcher $p+p'i$ nicht enthalten ist.

Offenbar ist von den reellen Zahlen $1, 2, 3 \ldots (p^2+p'^2-1)$ keine durch $p+p'i$ theilbar. Denn wäre b eine solche und $\frac{b}{p+p'i}$ eine ganze Zahl; so müsste auch $\frac{b(p-p'i)}{p^2+p'^2}=\frac{bp}{p^2+p'^2}$ $-\frac{bp'}{p^2+p'^2}i$ eine ganze Zahl sein. Da nun $p^2+p'^2$ eine reelle Primzahl ist, welche weder in b, noch in p, noch in p', also auch nicht in bp und nicht bp' aufgeht; so kann auch nicht $p+p'i$ in b enthalten sein.

Hieraus folgt auch, dass keine zwei Zahlen wie b und c aus der eben genannten Reihe nach dem Model $p+p'i$ einander kongruent sein können, weil sonst die Differenz $b-c$, welche derselben Reihe angehört, durch $p+p'i$ theilbar sein müsste.

II. Bildet man also sukzessive die Produkte aus $a+a'i$ und den reellen Zahlen $1, 2, 3 \ldots (p^2+p'^2-1)$, und nimmt von jedem dieser Produkte den kleinsten positiven Rest $b+b'i$; so werden alle diese Reste von einander verschieden, mithin gleich den in §. 207 ebenso bezeichneten, in dem Quadrate $OACB$ liegenden Zahlen sein.

III. Ferner ist klar, dass jede der in dem Quadrate $OACB$ liegenden komplexen Zahlen irgend Einer der reellen Zahlen aus der mehr erwähnten Reihe nach dem Model $p+p'i$ kongruent ist.

Demnach kann auch stets statt des kleinsten positiven komplexen Restes $b+b'i$, welcher irgend einer gegebenen Zahl $a+a'i$ nach dem Model $p+p'i$ kongruent ist und in dem Quadrate $OACB$ liegt, eine reelle Zahl A aus der Reihe $1, 2, 3 \ldots (p^2+p'^2-1)$ gefunden werden, welche ebenfalls der $a+a'i$ kongruent ist.

Das Letztere und zugleich die nähere Beschaffenheit der reellen Zahl A ergibt sich auch unmittelbar, wenn man die Möglichkeit der Kongruenz

(1) $$a+a'i \equiv A \bmod p+p'i$$

näher untersucht. Diese Kongruenz ist gleichbedeutend mit der Gleichung

$$a+a'i = A+(v+v'i((p+p'i)$$
$$= A+vp-vp'+(v'p+vp')i$$

welche in folgende zwei Gleichungen

(2) $a = A + vp - v'p'$ oder $A = a - vp + v'p'$

(3) $a' = v'p + vp'$

zerfällt. Da nun $p + p'i$ eine vollkommene und wirklich komplexe Primzahl ist, also p und p' relativ prim oder beide $= \pm 1$ sind; so gibt es stets ganze Werthe für v und v', welche die Gl. (3) erfüllen, und welche mithin nach Gl. (2) auch für A eine ganze Zahl ergeben. Diese ganze Zahl kann stets positiv und $< p^2 + p'^2$ gemacht werden, da, wenn $a + a'i \equiv A$ ist, auch $a + a'i \equiv A \pm w(p^2 + p'^2)$ ist; indem man $p^2 + p'^2 = (p - p'i)(p + p'i)$ hat.

Wenn der absolute Werth von p und p' gleich 1, also $p^2 + p'^2 = 2$ ist, kann A stets $= +1$ gemacht werden. In jedem anderen Falle ergibt sich, jenachdem man zwischen den beiden Gleichungen (2) und (3) die Grösse v' oder die Grösse v eliminirt, für A der Ausdruck

(4) $$A = \frac{1}{p}[ap + a'p' - v(p^2 + p'^2)] \quad \text{oder}$$

(5) $$A = \frac{1}{p'}[ap' - a'p + v'(p^2 + p'^2)]$$

IV. Behuf der Untersuchungen in §. 208 und 209 bildeten wir die Produkte aus der Zahl $a + a'i$ und den innerhalb des Quadrates $OACB$ liegenden komplexen Zahlen, deren Anzahl $p^2 + p'^2 - 1$ ist, und suchten die kleinsten positiven Reste dieser Produkte, worunter alle Zahlen desselben Quadrates zum Vorschein kommen mussten.

Bilden wir jetzt zu ähnlichem Zwecke die Produkte aus $a + a'i$ und den reellen Zahlen $1, 2, 3 \ldots (p^2 + p'^2 - 1)$, und nehmen wir die kleinsten positiven reellen Reste dieser Produkte; so müssen darunter alle eben genannten reellen Zahlen vorkommen. Diese Gruppe von Kongruenzen sei, indem wir den Fall $p^2 + p'^2 = 2$, wofür alle jene Reste $= 1$ werden, ausschliessen und zur Abkürzung die Norm $p^2 + p'^2$ des Models, welche alsdann eine reelle Primzahl von der Form $4n + 1$ ist, mit r bezeichnen,

(G)
$$\begin{aligned} 1(a + a'i) &\equiv A_1 \mod p + p'i \\ 2(a + a'i) &\equiv A_2 \\ 3(a + a'i) &\equiv A_3 \\ &\vdots \\ \frac{r-1}{2}(a + a'i) &\equiv A_{\frac{r-1}{2}} \\ &\vdots \\ (r-1)(a + a'i) &\equiv A_{r-1} \end{aligned}$$

Multiplizirt man alle diese Kongruenzen mit einander, und beachtet, dass das Produkt $1.2.3\ldots(r-1) \equiv A_1 A_2 \ldots A_{r-1}$ ist und dass in keinem Faktor dieses Produktes die vollkommene Primzahl $p+p'i$ enthalten ist, dass man also die entstehende Kongruenz mit jenem Produkte dividiren kann; so ergibt sich zuvörderst der erweiterte Fermatsche Lehrsatz (§. 208), nämlich

(6) $$(a+a'i)^{r-1} \equiv 1 \mod p+p'i$$

Betrachten wir jetzt die obere Hälfte der Kongruenzen der Gruppe (G). Angenommen, es kommen unter den Resten auf der rechten Seite derselben deren m vor, welche $> \frac{r}{2}$ sind. Offenbar kann, da $r = p^2+p'^2 = (p-p'i)(p+p'i)$ ist, für jeden Rest A dieser Art der Ausdruck $r-B$ oder der ihm kongruente Werth $-B$ gesetzt werden, worin nun B positiv und $< \frac{r}{2}$ ist. Nimmt man diese Substitution für jeden Rest der eben genannten Art vor; so werden unter den Grössen A und B auf der rechten Seite alle Zahlen $1, 2, 3 \ldots \frac{r-1}{2}$ erscheinen, von denen m negativ sind. Multiplizirt man also die ersten $\frac{r-1}{2}$ Kongruenzen mit einander und dividirt die entstehende Kongruenz durch $1.2.3\ldots\frac{r-1}{2}$; so kommt

(7) $$(a+a'i)^{\frac{r-1}{2}} \equiv (-1)^m \mod p+p'i$$

Diese Formel vertritt die Kongruenz (3) in §. 209.

Da allgemein n^2 und $(r-n)^2$ zwei reelle Zahlen sind, welche nach dem Model $r = p^2+p'^2$, also auch nach dem Model $p+p'i$ einander kongruent sind; so leuchtet ein, dass man bei der Untersuchung des §. 202, wo alle Werthe für $x+x'i$ gesucht werden, welche den Ausdruck $I = D+D'i-(x+x'i)^2$ durch $q+q'i$ theilbar machen, statt $x+x'i$ nach und nach die reellen Zahlen $1, 2, 3 \ldots \frac{q^2+q'^2-1}{2}$ substituiren kann, insofern $q+q'i$ wirklich komplex und eine vollkommene Primzahl ist. (Die Methode des §. 202 ist allgemein gültig und von den letzteren Bedingungen nicht abhängig.)

V. Nachdem man die reelle Zahl A_1 gefunden hat, welche $\equiv a+a'i$ nach dem Model $p+p'i$ ist, lassen sich die reellen Reste $A_2, A_3 \ldots A_n$ der sukzessiven Vielfachen von $a+a'i$ sehr leicht durch die Bildung von Kongruenzen aus lauter reellen Zahlen darstellen. Denn offenbar hat man für jeden späteren Rest A_n die Beziehung $A_n \equiv nA_1 \mod p+p'i$; es ist also $A_n - nA_1$

durch $p+p'i$ theilbar. Demnach muss aber auch, weil $p+p'i$ eine vollkommene Primzahl ist, $A_n - nA_1$ durch $p-p'i$, mithin durch $(p+p'i)(p-p'i) = p^2+p'^2$ theilbar sein; es muss also auch $A_n \equiv nA_1 \, mod\, p^2+p'^2$ sein.

Hiernach stellen die Grössen $A_1, A_2, A_3 \ldots$ die Reste der sukzessiven Vielfachen von A_1 nach dem reellen Model $p^2+p'^2 = r$ dar.

VI. Die vorstehende Bemerkung gibt ein Mittel, den Werth von $(-1)^m$ auf der rechten Seite der Kongruenz (7) aus reellen Zahlen zu bestimmen, ohne dass man nöthig hat, zuvörderst den reellen Rest A_1 von $a+a'i$ zu ermitteln. Denn zuvörderst ist klar, dass man auch hat

$$(8) \qquad A^{\frac{r-1}{2}} \equiv (-1)^m \, mod\, r$$

Hierin und in (7) hat die Grösse m denselben Werth und $A = A_1$ bezeichnet den reellen Rest von $a+a'i$, welcher nach der Formel (4) oder (5) zusammengesetzt ist.

Verstehen wir also unter dem Ausdrucke $a\, mod\, p$ den absolut kleinsten Rest von a nach dem Model p, sodass die Formel

$$a\, mod\, p = b\, mod\, q$$

ausdrückt, dass der absolut kleinste Rest von a nach dem Model p gleich dem absolut kleinsten Reste von b nach dem Model q sei; so haben wir nach (7) und (8)

$$(9) \qquad (a+a'i)^{\frac{r-1}{2}} \, mod\, p+p'i = A^{\frac{r-1}{2}} \, mod\, r$$

Von den beiden Zahlen p, p' ist die Eine paar, die andere unpaar. Angenommen, p sei unpaar. Alsdann sind alle Faktoren von p unpaar. Setzt man nun $p = bcd \ldots$, sodass $b, c, d \ldots$ alle gleichen und ungleichen Primfaktoren von p darstellen; so hat man

$$r = p^2 + p'^2 = p'^2 + (bcd\ldots)(bcd\ldots)$$

Hiernach ist r ein quadratischer Rest nach jeder der Primzahlen $b, c, d \ldots$ Da diese Primzahlen ebenso wie r unpaar sind, und ausserdem r die Form $4n+1$ besitzt; so ist nach dem Fundamentalsatze für die quadratischen Reste (§. 149) auch umgekehrt jede der Zahlen $b, c, d \ldots$ ein quadratischer Rest nach r, und demzufolge

$$b^{\frac{r-1}{2}} \equiv 1 \, mod\, r, \qquad c^{\frac{r-1}{2}} \equiv 1 \, mod\, r, \qquad d^{\frac{r-1}{2}} \equiv 1 \, mod\, r \text{ etc.}$$

Multiplizirt man alle diese Kongruenzen mit einander; so kommt, da $bcd \ldots = p$ ist,

$$(10) \qquad p^{\frac{r-1}{2}} \equiv 1 \, mod\, r$$

Hiernach ist auch

(11) $$A^{\frac{r-1}{2}} \equiv (pA)^{\frac{r-1}{2}} \mod r$$

Nach Gl. (4) hat man aber

$$pA = ap + a'p' - vr \equiv ap + a'p' \mod r$$

folglich ist

(12) $$A^{\frac{r-1}{2}} \equiv (ap + a'p')^{\frac{r-1}{2}} \mod r$$

und mithin auch wegen (8)

(13) $$(ap + a'p')^{\frac{r-1}{2}} \equiv (-1)^m \mod r$$

oder wegen (9)

(14) $$(a + a'i)^{\frac{r-1}{2}} \mod p + p'i = (ap + a'p')^{\frac{r-1}{2}} \mod r$$

Um also zu entscheiden, ob $(a + a'i)^{\frac{r-1}{2}} \equiv +1$ oder -1 nach dem Model $p + p'i$ ist, braucht man nur zu untersuchen, ob $(ap + a'p')^{\frac{r-1}{2}} \equiv +1$ oder -1 nach dem Model r ist.

Wäre p paar, also p' unpaar; so fände man auf demselben Wege statt (10) die Beziehung

(15) $$p'^{\frac{r-1}{2}} \equiv 1 \mod r$$

und mit Hülfe der Gl. (5) statt (13) und (14) resp.

(16) $$(ap' - a'p)^{\frac{r-1}{2}} \equiv (-1)^m \mod r$$

(17) $$(a + a'i)^{\frac{r-1}{2}} \mod p + p'i = (ap' - a'p)^{\frac{r-1}{2}} \mod r$$

Will man es gleichgültig lassen, ob p oder p' die unpaare Zahl ist; so nehme man allgemein an, der Faktor 2 sei in p überhaupt ϱ mal und in p' überhaupt ϱ' mal enthalten. Es sei also

$$p = 2^{\varrho} bcd \ldots, \qquad p' = 2^{\varrho'} bcd \ldots$$

worin stets entweder ϱ oder ϱ' gleich null sein wird.

Für die unpaaren Faktoren $b, c, d \ldots$ gelten immer die obigen Kongruenzen. Was den Faktor 2 betrifft; so hat man nach §. 148, XIII.

$$2^{\frac{r-1}{2}} \equiv (-1)^{\frac{r-1}{4}} \mod r \qquad \text{also}$$

$$2^{\frac{\varrho(r-1)}{2}} \equiv (-1)^{\frac{\varrho(r-1)}{4}} \mod r$$

$$2^{\frac{\varrho'(r-1)}{2}} \equiv (-1)^{\frac{\varrho'(r-1)}{4}} \mod r$$

Hiernach ist

$$(18) \qquad p^{\frac{r-1}{2}} \equiv (-1)^{\frac{\varrho(r-1)}{4}} \mod r$$

$$(19) \qquad p'^{\frac{r-1}{2}} \equiv (-1)^{\frac{\varrho'(r-1)}{4}} \mod r$$

mithin

$$A^{\frac{r-1}{2}} \equiv (-1)^{\frac{\varrho(r-1)}{4}} (pA)^{\frac{r-1}{2}} \equiv (-1)^{\frac{\varrho'(r-1)}{4}} (p'A)^{\frac{r-1}{2}} \mod r$$

Hieraus und aus (4), (5), (9) ergibt sich die Doppelbeziehung

$$(20) \qquad (a+a'i)^{\frac{r-1}{2}} \mod p+p'i =$$

$$(-1)^{\frac{\varrho(r-1)}{4}} \left[(ap+a'p')^{\frac{r-1}{2}} \mod r\right] = (-1)^{\frac{\varrho'(r-1)}{4}} \left[(ap'-a'p)^{\frac{r-1}{2}} \mod r\right]$$

Bei den vorstehenden Untersuchungen war nur die Bedingung gestellt, dass der Model $p+p'i$ wirklich komplex sei. Die Zahl $a+a'i$ kann dagegen auch reell oder rein imaginär sein. Ist $a+a'i$ reell, also $a'=0$; so erhält man aus (20) unter Berücksichtigung der Beziehungen (18), (19)

$$(21) \qquad a^{\frac{r-1}{2}} \mod p+p'i = a^{\frac{r-1}{2}} \mod r$$

Ist $a+a'i$ rein imaginär, also $a=0$; so erhält man

$$(22) \qquad (a'i)^{\frac{r-1}{2}} \mod p+p'i = (-1)^{\frac{(\varrho+\varrho')(r-1)}{4}} \left[a'^{\frac{r-1}{2}} \mod r\right]$$

VII. Betrachten wir jetzt den Fall, wo der Model $p+p'i$ reell oder rein imaginär, wo also $p'=0$ oder $p=0$ ist. Der absolute Werth dieses Models, welcher stets als vollkommen prim vorausgesetzt wird, ist alsdann von der Form $4n+3$.

Jetzt ist es nach Ansicht der Gleichungen (2) und (3) offenbar nicht in allen Fällen möglich, eine reelle Zahl A zu ermitteln, welche nach dem gegenwärtigen Model kongruent zu $a+a'i$ sei.

Auch findet hier die Betrachtung sub I. keine Anwendung, indem die Zahlen 1, 2, 3 ... $(p^2+p'^2-1)$ nicht sämmtlich inkongruent nach dem jetzigen Model sind.

Immer aber ist es möglich, den Rest der Potenz $(a+a'i)^{\frac{1}{2}(p^2+p'^2-1)} = (a+a'i)^{\frac{r-1}{2}}$, welcher bekanntlich $=\pm 1$ und vorhin mit $(-1)^m$ bezeichnet ist, aus reellen Zahlen zu bestimmen. Nehmen wir zu dem Ende an, es sei $p'=0$, also der Model reell $=p$ und $r=p^2+p'^2=p^2$. (Der andere Fall, wo der Model rein imaginär ist, führt zu demselben Resultate, wenn man unter p den absoluten Werth des Models versteht, da jede zwei nach p kongruente Zahlen auch nach pi kongruent sind.)

Nach §. 135, XVIII. hat man, in Berücksichtigung, dass p die Form $4n+3$ hat, also $i^p = -i$ ist,

$$(a+a'i)^p \equiv a^p + (a'i)^p \equiv a^p - a'^p i \bmod p$$

Immer ist nun $a^p \equiv a$ und $a'^p \equiv a'$. Denn geht p in a, resp. in a' auf; so ist Dies ohne Weiteres klar. Geht aber p in a, resp. in a' nicht auf; so erkennt man die Richtigkeit aus dem Fermatschen Lehrsatze $a^{p-1} \equiv 1$, resp. $a'^{p-1} \equiv 1$. Demnach hat man

(23) $$(a+a'i)^p \equiv a - a'i \bmod p$$

Multiplizirt man diese Kongruenz auf beiden Seiten mit $a+a'i$; so kommt

(24) $$(a+a'i)^{p+1} \equiv a^2 + a'^2 \bmod p$$

also, wenn man auf die Potenz vom Grade $\frac{p-1}{2}$ erhebt,

(25) $$(a+a'i)^{\frac{p^2-1}{2}} \equiv (a^2+a'^2)^{\frac{p-1}{2}} \bmod p$$

Hierin besteht die gesuchte Beziehung, mittelst welcher man den Rest $(-1)^m$ in (7) aus lauter reellen Zahlen bestimmen kann.

Es muss hierbei bemerkt werden, dass wenn p negativ reell, sowie auch dann, wenn diese Zahl positiv oder negativ rein imaginär ist, nur im Exponenten $\frac{p-1}{2}$ auf der rechten Seite der Kongruenz (25) für p der absolute Werth dieses Models zu nehmen ist.

§. 213. Das Reziprozitätsgesetz für komplexe Zahlen.

I. Es seien $p+p'i$ und $q+q'i$ zwei wirklich komplexe, vollkommene und nicht bloss durch den Faktor i, i^2 oder i^3 von einander verschiedene Primzahlen von unpaaren Normen. In beiden seien die reellen Theile p und q unpaar und die imaginären Theile oder p' und q' paar. Setzt man die Normen

$$r = p^2 + p'^2, \qquad s = q^2 + q'^2$$

sodass r und s zwei positive reelle Primzahlen von der Form $4n+1$ darstellen; so besteht das Reziprozitätsgesetz (§. 143) darin, dass man gleichzeitig

(1) $$(q+q'i)^{\frac{r-1}{2}} \equiv (-1)^m \bmod p + p'i$$

(2) $$(p+p'i)^{\frac{s-1}{2}} \equiv (-1)^m \bmod q + q'i$$

oder

$$(3) \qquad (q+q'i)^{\frac{r-1}{2}} \bmod p+p'i \equiv (p+p'i)^{\frac{s-1}{2}} \bmod q+q'i$$

hat, eine Beziehung, welche man analog der von Legendre für reelle Zahlen angewandten Bezeichnung (§. 148, IX.) auch folgendermaassen schreiben kann:

$$(3^a) \qquad \left(\frac{q+q'i}{p+p'i}\right)=\left(\frac{p+p'i}{q+q'i}\right)$$

Denn man hat

$$(pq+p'q')^2+(p'q-pq')^2=(p^2+p'^2)(q^2+q'^2)=rs$$

Hierin ist die Grösse $pq+p'q'$ entschieden unpaar, und hat demnach nur unpaare Faktoren. Setzt man also $pq+p'q'=bcd\ldots$, worin $b, c, d\ldots$ lauter Primzahlen bedeuten; so ist aus der Formel

$$rs=(p'q-pq')^2+(bcd\ldots)(bcd\ldots)$$

klar, dass die Zahl rs ein quadratischer Rest nach jeder der Zahlen $b, c, d\ldots$ ist. Demnach muss laut §. 151, I., sowol r, als auch s gleichzeitig ein quadratischer Rest oder es muss sowol r, als auch s gleichzeitig ein quadratischer Nichtrest nach b, nach c, nach d u. s. w. sein.

Da nun r und s Primzahlen von der Form $4n+1$ sind; so muss nach dem Fundamentalsatze für die quadratischen Reste (§. 149) auch umgekehrt jede der Zahlen $b, c, d\ldots$ in derselben Beziehung zu r stehen, in welcher sie zu s steht, d. h. entweder gleichzeitig nach r und s ein quadratischer Rest oder nach r und s ein quadratischer Nichtrest sein. Demnach kann man schreiben

$$b^{\frac{r-1}{2}} \equiv (-1)^\beta \bmod r \quad \text{und} \quad b^{\frac{s-1}{2}} \equiv (-1)^\beta \bmod s$$
$$c^{\frac{r-1}{2}} \equiv (-1)^\gamma \bmod r \qquad\quad c^{\frac{s-1}{2}} \equiv (-1)^\gamma \bmod s$$
$$\text{etc.} \qquad\qquad\qquad \text{etc.}$$

Multiplizirt man die links stehenden und auch die rechts stehenden Kongruenzen für sich; so kommt, da $bcd\ldots=pq+p'q'$ ist,

$$(4) \qquad (pq+p'q')^{\frac{r-1}{2}} \bmod r \equiv (pq+p'q')^{\frac{s-1}{2}} \bmod s$$

Berücksichtigt man nun, dass nach dem vorhergehenden Paragraphen, Gl. (14)

$$(q+q'i)^{\frac{r-1}{2}} \bmod p+p'i \equiv (pq+p'q')^{\frac{r-1}{2}} \bmod r$$
$$(p+p'i)^{\frac{s-1}{2}} \bmod q+q'i \equiv (pq+p'q')^{\frac{s-1}{2}} \bmod s$$

ist; so erkennt man, dass die Gl. (4) mit der zu beweisenden Gl. (3) identisch ist.

II. Das obige Reziprozitätsgesetz behält auch dann Gültigkeit, wenn die Eine Primzahl $p + p'i$ komplex, die andere dagegen reell $= q$ (also unpaar und, absolut genommen, von der Form $4n + 3$) ist.

Behalten wir die frühere Bezeichnung bei, sodass nun $r = p^2 + p'^2$ eine Primzahl von der Form $4n + 1$, und $s = q^2$ das Quadrat einer in der Form $4n + 3$ enthaltenen Primzahl, also selbst eine Zahl von der Form $4n + 1$ ist; so ist statt der Gl. (3) die Gleichung

$$(5) \qquad q^{\frac{r-1}{2}} \bmod p + p'i = (p + p'i)^{\frac{s-1}{2}} \bmod q$$

zu beweisen.

Dieser Nachweis ergibt sich aus dem vorhergehenden Paragraphen, indem man nach der dortigen Gl. (21)

$$q^{\frac{r-1}{2}} \bmod p + p'i = q^{\frac{r-1}{2}} \bmod r$$

und nach der dortigen Gl. (25)

$$(p + p'i)^{\frac{s-1}{2}} \bmod q = (p^2 + p'^2)^{\frac{q-1}{2}} \bmod q = r^{\frac{q-1}{2}} \bmod q$$

hat. Beachtet man jetzt, dass die Primzahl r von der Form $4n + 1$ ist; so folgt aus dem Reziprozitätsgesetze für reelle Zahlen (§. 148)

$$q^{\frac{r-1}{2}} \bmod r = r^{\frac{q-1}{2}} \bmod q$$

was unter Berücksichtigung der vorhergehenden beiden Gleichungen die Richtigkeit der Formel (5) erkennen lässt. (Ist q negativ; so ist nur im Exponenten $\frac{q-1}{2}$ auf der rechten Seite der letzten und vorletzten Kongruenz der absolute Werth von q zu verstehen. Auf die Gl. (5) hat Dies keinen Einfluss.)

III. Endlich gilt das obige Reziprozitätsgesetz auch für den Fall, wo beide Primzahlen reell $= p$ und q (also beide unpaar und, absolut genommen, von der Form $4n + 3$) sind.

Wir haben jetzt $r = p^2$ und $s = q^2$, sodass beide Zahlen Quadrate von der Form $4n + 1$ sind. Statt Gl. (3) ist die folgende

$$(6) \qquad q^{\frac{r-1}{2}} \bmod p = p^{\frac{s-1}{2}} \bmod q = 1$$

zu beweisen. Die Richtigkeit dieser Gleichung leuchtet ein, wenn man beachtet, dass nach dem Fermatschen Lehrsatze

$$q^{p-1} \equiv 1 \bmod p \qquad \text{also auch}$$

$$q^{\frac{(p+1)(p-1)}{2}} = q^{\frac{p^2-1}{2}} = q^{\frac{r-1}{2}} \equiv 1 \bmod p$$

und ebenso $p^{\frac{s-1}{2}} \equiv 1 \bmod q$ ist.

(Wäre p oder q oder beide negativ; so hätte man nur in den Exponenten der letzteren Kongruenzen unter p und q deren absolute Werthe zu verstehen, was auf die Kongruenz (6) ohne Einfluss ist.)

Man sieht, dass die beiden Formeln (5) und (6) in der allgemeineren (3) als spezielle Fälle enthalten sind.

IV. Um die Beziehungen darzustellen, welche sich ergeben, wenn der reelle Theil der Einen oder der anderen jener beiden Primzahlen paar ist; so bezeichne man mit p und q stets unpaare und mit p' und q' stets paare Zahlen, welche letzteren auch $=0$ sein können. Alle diese Zahlen können positiv oder negativ sein. Die früher mit r und s bezeichneten Zahlen behalten immer denselben Werth und sind stets positive Zahlen von der Form $4n+1$.

Es leuchtet ein, dass zwei Zahlen, welche nach irgend einem Model kongruent sind, es auch nach einem Model sein werden, welcher das Produkt aus jenem und irgend einer Potenz von i darstellt.

Hat nun die Eine Primzahl die Form $p'+pi$; so kann man setzen $i(p'+pi) = -p+p'i$. Da $\frac{s-1}{2}$ eine paare Zahl $=2.\frac{s-1}{4}$ ist; so hat man

$$(-p+p'i)^{\frac{s-1}{2}} = (-1)^{\frac{s-1}{4}}(p'+pi)^{\frac{s-1}{2}}$$

Nach (3) ist aber

$$(q+q'i)^{\frac{r-1}{2}} \bmod -p+p'i = (-p+p'i)^{\frac{s-1}{2}} \bmod q+q'i$$

Substituirt man auf der rechten Seite für $(-p+p'i)^{\frac{s-1}{2}}$ den so eben gefundenen gleichen Werth und verwandelt auf der linken Seite den Model $-p+p'i$ in den Model $-i(-p+p'i) = p'+pi$, was nach der Vorbemerkung zulässig ist; so ergibt sich, wenn nur in der Einen Primzahl $p'+pi$ der reelle Theil paar ist,

$$(7) \quad (q+q'i)^{\frac{r-1}{2}} \bmod p'+pi = (-1)^{\frac{s-1}{4}}\left[(p'+pi)^{\frac{s-1}{2}} \bmod q+q'i\right]$$

Ebenso erhält man, wenn nur in der anderen Primzahl $q'+qi$ der reelle Theil paar ist,

(8) $$(-1)^{\frac{r-1}{4}}\left[(q'+qi)^{\frac{r-1}{2}} \bmod p+p'i\right]=(p+p'i)^{\frac{s-1}{2}} \bmod (q'+qi)$$

und wenn in beiden Primzahlen die reellen Theile paar sind,

(9) $$(-1)^{\frac{r-1}{4}}\left[(q'+qi)^{\frac{r-1}{2}} \bmod p'+pi\right]=(-1)^{\frac{s-1}{4}}\left[(p'+pi)^{\frac{s-1}{2}} \bmod q'+qi\right]$$

V. Was den Fall betrifft, wo die Norm der Einen oder der anderen der in Rede stehenden Primzahlen $=2$ ist; so kann offenbar nur Eine jener Primzahlen diese Norm besitzen. Denn wäre die Norm einer jeden $=2$; so unterschieden sie sich lediglich durch eine Potenz von i von einander, was der allgemeinen Bedingung ad I. nicht gemäss sein würde.

Ist also nur die Eine Primzahl $p+p'i=1+i$ oder das Negative davon; so weiss man aus dem vorhergehenden Paragraphen Nr. IV., dass jede beliebige Potenz irgend einer Zahl $q+q'i$, in welcher $1+i$ nicht aufgeht, den Rest 1 nach dem Model $1+i$ besitzt. Man hat also allgemein

(10) $$q+q'i\equiv 1 \bmod 1+i$$

Umgekehrt ergeben sich die Reste der Potenzen von $1\pm i$ nach dem Model $q+q'i$ zuvörderst für den Fall, wo dieser Model wirklich komplex ist, aus Gl. (14) des vorhergehenden Paragraphen. Danach hat man, wenn q unpaar und q' paar ist,

(11) $$(1\pm i)^{\frac{s-1}{2}} \bmod q+q'i=(q\pm q')^{\frac{s-1}{2}} \bmod s$$

Hierin sind links und rechts gleichzeitig die oberen oder die unteren Zeichen zu nehmen, und auf der rechten Seite ändert sich Nichts, wenn der reelle Theil von $1\pm i$ sich in -1 verwandelt.

Die vorstehende Formel lässt sich noch weiter vereinfachen, wenn man beachtet, dass

$$(q\pm q')^2+(q\mp q')^2=2(q^2+q'^2)=2s$$

ist. Da $q+q'i$ nicht durch $1+i$ theilbar sein soll; so muss von den beiden Zahlen q und q' stets die Eine paar, die andere unpaar, und $q\pm q'$ stets unpaar sein. Setzt man nun $q\pm q'=bcd\ldots$, worin $b, c, d\ldots$ lauter Primzahlen bezeichnen, welche sämmtlich unpaar sind; so hat man

$$2s=(q\pm q')^2+(bcd\ldots)(bcd\ldots)$$

Hiernach ist $2s$ ein quadratischer Rest nach jeder der Zahlen $b, c, d\ldots$ Demnach ist sowol die Zahl 2, als auch die Zahl s gleichzeitig entweder ein quadratischer Rest oder ein quadratischer Nichtrest nach b, nach c, nach d u. s. w. Setzt man also

$$2^{\frac{b-1}{2}} \equiv (-1)^{\beta} \bmod b; \text{ so ist auch } s^{\frac{b-1}{2}} \equiv (-1)^{\beta} \bmod b$$

$$2^{\frac{c-1}{2}} \equiv (-1)^{\gamma} \bmod c \quad » \quad » \quad » \quad s^{\frac{c-1}{2}} \equiv (-1)^{\gamma} \bmod c$$

u. s. w.

Nach §. 148, XIII. hat man wegen der links stehenden Kongruenzen für $\beta, \gamma, \delta \ldots$ die in den Ausdrücken $b = 4\beta \pm 1$, $c = 4\gamma \pm 1$, $d = 4\delta \pm 1$ u. s. w. erscheinenden Werthe zu nehmen.

Was die rechts stehenden Kongruenzen betrifft; so ist, da die reelle Primzahl $s = q^2 + q'^2$ die Form $4m + 1$ besitzt, nach dem Reziprozitätsgesetze (§. 148) auch umgekehrt

$$b^{\frac{s-1}{2}} \equiv (-1)^{\beta} \bmod s$$

$$c^{\frac{s-1}{2}} \equiv (-1)^{\gamma} \bmod s$$

u. s. w.

also wenn man alle diese Kongruenzen multiplizirt, und beachtet, dass $bcd \ldots = q \pm q'$ ist,

$$(q \pm q')^{\frac{s-1}{2}} \equiv (-1)^{\beta+\gamma+\delta+\cdots} \bmod s$$

Setzt man nun den absoluten Werth von $q \pm q' = 4n \pm 1$; so hat man, da auch $q \pm q' = (4\beta \pm 1)(4\gamma \pm 1)(4\delta \pm 1) \ldots = 4(2m \pm \beta \pm \gamma \pm \delta \pm \ldots) \pm 1$ ist, $n = 2m \pm \beta \pm \gamma \pm \delta \pm \ldots$, worin vor den Zahlen $\beta, \gamma, \delta \ldots$ und 1 ganz beliebige Zeichen stehen können. Hieraus ist klar, dass die beiden Zahlen n und $(\beta + \gamma + \delta + \ldots)$ stets gleichzeitig paar oder gleichzeitig unpaar sind. Demnach kann man statt der vorstehenden Kongruenz auch schreiben

$$(12) \qquad (q \pm q')^{\frac{s-1}{2}} \equiv (-1)^{n} \bmod s$$

Hiernach hat man statt (11) die Beziehung

$$(13) \qquad (1 \pm i)^{\frac{s-1}{2}} \equiv (-1)^{n} \bmod q + q'i$$

und es ist, wenn links der Werth $1 + i$ gilt, der absolute Werth von $q + q' = 4n \pm 1$, und wenn links der Werth $1 - i$ gilt, der absolute Werth von $q - q' = 4n \pm 1$ zu setzen.

Ist der Model $= q' + qi$, also dessen reeller Theil paar und dessen imaginärer unpaar; so hat man nach Gl. (17) des vorhergehenden Paragraphen

$$(14) \qquad (1 \pm i)^{\frac{s-1}{2}} \bmod q' + qi = (q \mp q')^{\frac{s-1}{2}} \bmod s$$

und es findet sich statt (13)

$$(15)\qquad (1 \pm i)^{\frac{s-1}{2}} \equiv (-1)^n \bmod q' + qi$$

Hierin ist, wenn links der Werth $1+i$ gilt, der absolute Werth von $q - q' = 4n \pm 1$, und wenn links der Werth $1 - i$ gilt, der absolute Werth von $q + q' = 4n \pm 1$ zu setzen. Die Verwandlung des reellen Theiles von $1 \pm i$ in -1 auf der linken Seite ändert die rechte Seite nicht.

Für den Fall, wo der Model $q + q'i$ reell $= q$, also sein absoluter Werth von der Form $4n - 1$ ist, ergibt zunächst die Formel (25) des vorhergehenden Paragraphen

$$(1 \pm i)^{\frac{s-1}{2}} \equiv 2^{\frac{q-1}{2}} \bmod q$$

und alsdann die Formel (15) und (16) des §. 148

$$(16)\qquad (1 \pm i)^{\frac{s-1}{2}} \equiv (-1)^n \bmod q$$

Auch hierin kann der reelle Theil von $1 \pm i$ in -1 verwandelt werden.

Man sieht, dass die Formel (16) als ein spezieller Fall der Formel (13) angesehen werden kann, wenn man in dieser $q' = 0$ setzt.

VI. Endlich bemerken wir für den Fall, wo $p + p'i = \pm i$ sein sollte, dass wenn man die Norm der anderen Primzahl $q + q'i$, also $q^2 + q'^2 = 4n + 1$ setzt,

$$(17)\qquad (\pm i)^{\frac{s-1}{2}} \equiv (-1)^n \bmod q + q'i$$

sein wird, gleichviel ob der Model komplex ist oder nicht.

Wäre der Model $q + q'i = 1 \pm i$; so ist jede Potenz von $\pm i$ sowol $\equiv 1$, als auch $\equiv -1$.

§. 214. *Der Fundamentalsatz für die Theorie der quadratischen Reste für komplexe Zahlen.*

I. Aus dem Reziprozitätsgesetze des vorhergehenden Paragraphen Nr. I., II., III., wovon die dortige Formel (3) der allgemeine Repräsentant ist, ergibt sich mit Hülfe des §. 211, II. sofort die Erweiterung des Gauss'schen Fundamentalsatzes, welcher in §. 149 für reelle Zahlen erläutert ist.

Wenn nämlich $p + p'i$ und $q + q'i$ zwei vollkommene und nicht bloss durch den Faktor i, i^2 oder i^3 von einander verschiedene Primzahlen von unpaaren Normen sind, und in welchen die reellen Theile p und q unpaar sind (wobei die imaginären Theile auch den Werth null besitzen können); so ist die erste ein quadratischer Rest oder Nichtrest nach der zweiten, wenn

die zweite resp. ein quadratischer Rest oder Nichtrest nach der ersten ist. Man hat also

(1) $(p+p'i)R(q+q'i)$ wenn $(q+q'i)R(p+p'i)$ ist

(2) $(p+p'i)N(q+q'i)$ » $(q+q'i)N(p+p'i)$ »

Aus der Formel (6) des vorhergehenden Paragraphen ergibt sich für den speziellen Fall, wo beide Primzahlen reell, also absolut genommen, von der Form $4n+3$ sind, dass jede Primzahl p quadratischer Rest nach jeder Primzahl q ist.

II. Wenn in Einer der obigen Primzahlen oder in beiden der reelle Theil paar ist; so ergeben die Formeln (7) und (9) des vorhergehenden Paragraphen leicht die gesuchten Beziehungen. Diese und das eben gefundene Resultat sind in der folgenden Tabelle zusammengestellt. Es bedeuten darin p und q unpaare, dagegen p' und q' paare Zahlen. Wo in den Spalten für die Normen $r=p^2+p'^2$ und $s=q^2+q'^2$ die einfachen Buchstaben r und s selbst gesetzt sind, ist es gleichgültig, ob diese Normen die Form $8n+1$ oder $8n+5$ haben.

P	Q	r	s		
$p+p'i$	$q+q'i$	r	s	QRP	PRQ
$p+p'i$	$q'+qi$	r	$8n+1$	QRP	PRQ
		r	$8n+5$	QRP	PNQ
$p'+pi$	$q'+qi$	$8m+1$	$8n+1$	QRP	PRQ
		$8m+5$	$8n+5$		
		$8m+1$	$8n+5$	QRP	PNQ
		$8m+5$	$8n+1$		

Das Stattfinden der Einen der beiden rechts neben einander stehenden Beziehungen bedingt immer nothwendig die andere. Man kann übrigens in diesen Beziehungen in jeder Horizontalreihe das Symbol R in N und gleichzeitig das Symbol N in R verwandeln.

III. Dass man in einer Beziehung wie QRP oder QNP den Model P nach Belieben mit -1 und auch mit $\pm i$ multipliziren kann, ohne dass sich jene Beziehung ändert, leuchtet ein.

Ebenso kann man Q mit -1 multipliziren.

Multiplizirt man jedoch Q mit $\pm i$; so hat Dies nur dann keinen Einfluss auf jene Beziehung, wenn die Norm des Models

P, also $r = p^2 + p'^2$ von der Form $8m+1$ ist. Sobald jedoch diese Norm r von der Form $8m+5$ ist, ändert sich jene Beziehung, und es ist N statt R oder R statt N zu setzen.

IV. Es ist leicht zu zeigen, dass

wenn $q+q'iRp+p'i$ ist, auch $q-q'iRp-p'i$

sein wird, gleichviel ob die reellen Theile paar oder unpaar sind. Hierin kann auch N statt R gesetzt werden.

Multiplizirt man in der letzteren Beziehung $q-q'i$ und $p-p'i$ mit i; so ergibt sich folgender Satz.

Wenn die Norm r des Models $p+p'i$ die Form $8m+1$ hat, folgt aus der Beziehung

$$q+q'iRp+p'i \quad \text{auch} \quad q'+qiRp'+pi$$

Hat dagegen r die Form $8m+5$; so folgt aus

$$q+q'iRp+p'i \quad \text{stets} \quad q'+qiNp'+pi$$

In den letzteren Beziehungen kann auch R mit N und gleichzeitig N mit R vertauscht werden.

V. Wenn Eine der beiden Primzahlen die Norm 2 hat; so erkennt man sofort aus der Formel (10) des vorhergehenden Paragraphen, dass jede Primzahl $q+q'i$ quadratischer Rest nach $1\pm i$ ist, dass man also

$$(3) \qquad (q+q'i)R(1\pm i)$$

hat.

Umgekehrt folgt aus der Formel (13) des vorhergehenden Paragraphen, welche auch die dortige Formel (16) mit einschliesst, dass wenn in der Primzahl $q+q'i$ der reelle Theil q unpaar, dagegen q' paar (auch $=0$) ist, $(1\pm i)^{\frac{s-1}{2}} \equiv 1 \bmod q+q'i$ sein wird, wenn n eine paare Zahl ist. Das Letztere ereignet sich, wenn in dem absoluten Werthe $4n\pm 1$ von $q+q'$, resp. $q-q'$, die Grösse n paar ist, wenn also dieser Werth der Form $8n\pm 1$, d. h. entweder der Form $8n+1$ oder der Form $8n+7$ entspricht. Demnach hat man

(4) $(1\pm i)R(q+q'i)$, wenn absolut $q\pm q'=8n+1$ oder $8n+7$ ist,

(5) $(1\pm i)N(q+q'i)$ » » $q\pm q'=8n+3$ » $8n+5$ »

worin gleichzeitig die oberen oder die unteren Zeichen gelten.

Ist dagegen der reelle Theil des Models paar; so hat man nach der Formel (15) des vorhergehenden Paragraphen

(6) $(1\pm i)R(q'+qi)$, wenn absolut $q\mp q'=8n+1$ oder $8n+7$ ist,

(7) $(1\pm i)N(q'+qi)$ » » $q\mp q'=8n+3$ » $8n+5$ »

worin ebenfalls gleichzeitig die oberen oder die unteren Zeichen gelten.

VI. Endlich bemerken wir noch, dass man stets

(8) $$\pm 1 R q + q'i$$

hat. Dagegen ist nach der Formel (17) des vorhergehenden Paragraphen, wenn die Norm von $q+q'i$, also $q^2+q'^2=s$ gesetzt wird,

(9) $$\pm i R q + q'i, \text{ wenn } s = 8n+1$$

(10) $$\pm i N q + q'i \quad \text{»} \quad s = 8n+5$$

In diesen Formeln ist es gleichgültig, ob der reelle Theil des Models paar oder unpaar ist.

§. 215. *Die quadratischen Reste nach zusammengesetzten Modeln.*

A. Wenn $q+q'i$ von unpaarer Norm und relativ prim zu $D+D'i$ ist.

I. Für die Auflösung der unbestimmten Gleichungen vom zweiten Grade, §. 202, ist es von Wichtigkeit, leicht darüber entscheiden zu können, ob es Zahlen von der Form $D+D'i-(x+x'i)^2$ gebe, welche durch $q+q'i$ theilbar seien oder nicht, d. h. ob die Kongruenz

(1) $$D+D'i \equiv (x+x'i)^2 \bmod q+q'i$$

möglich oder unmöglich, oder ob $D+D'i$ ein quadratischer Rest oder Nichtrest nach $q+q'i$ sei.

Die je nach der Zusammensetzung des Models $q+q'i$ sich ergebenden Resultate sind denen in §. 150 analog und sollen im Folgenden vorgetragen werden.

Vorweg bemerken wir jedoch, dass in allen Formeln dieses Paragraphen der Model $q+q'i$, unbeschadet des Resultats, mit jeder beliebigen Potenz von i multiplizirt werden kann.

Wenn $q+q'i$ eine in $D+D'i$ nicht aufgehende vollkommene Primzahl von unpaarer Norm ist; so wird nach §. 211 der Bestand der Kongruenz (1) bedingt durch den Bestand der Kongruenz

(2) $$(D+D'i)^{\frac{1}{2}(q^2+q'^2-1)} \equiv 1 \bmod q+q'i$$

II. Wenn $q+q'i$ eine Potenz einer in $D+D'i$ nicht aufgehenden Primzahl von unpaarer Norm, also $=(r+r'i)^m$ ist; so ist $D+D'i$ dann, aber auch nur dann ein quadratischer Rest nach $q+q'i$, wenn es ein solcher nach dem Primfaktor $r+r'i$ ist, wenn man also hat

(3) $$(D+D'i)^{\frac{1}{2}(r^2+r'^2-1)} \equiv 1 \bmod r+r'i$$

Der Beweis ist wie in §. 150, II. zu führen, indem man beachtet, dass $2=(1+i)^2 i^3$ ist.

III. Wenn $q+q'i$ das Produkt mehrerer in $D+D'i$ nicht aufgehender verschiedener Primzahlen von unpaaren Normen oder auch das Produkt von Potenzen solcher Primzahlen, also $=(r+r'i)^m(s+s'i)^n\ldots$ ist; so ist $D+D'i$ dann, aber auch nur dann ein quadratischer Rest nach $q+q'i$, wenn es ein solcher nach jedem einzelnen der Primfaktoren $r+r'i$, $s+s'i\ldots$ ist, wenn man also hat

$$(4) \qquad (D+D'i)^{\frac{1}{2}(r^2+r'^2-1)} \equiv 1 \; mod\, r+r'i$$

$$(5) \qquad (D+D'i)^{\frac{1}{2}(s^2+s'^2-1)} \equiv 1 \; mod\, s+s'i$$

etc.

Der Beweis ist wie in §. 150, III. zu führen.

B. Wenn $q+q'i$ eine Potenz von $1+i$, aber relativ prim zu $D+D'i$ ist.

IV. Wenn $q+q'i=1+i$; so ist jeder Werth von $D+D'i$, auch wenn derselbe nicht relativ prim zu $q+q'i$ ist, quadratischer Rest nach $q+q'i$. Es ist also allgemein

$$(6) \qquad D+D'i \equiv (x+x'i)^2 \; mod\, 1+i$$

Denn ist $D+D'i$ durch $1+i$ theilbar; so ist, wenn $v+v'i$ beliebig gewählt und

$$D+D'i=[(1+i)(v+v'i)]^2+y+y'i$$

gesetzt wird, $y+y'i$ durch $1+i$ theilbar, also $=(1+i)(w+w'i)$, mithin

$$D+D'i=[(1+i)(v+v'i)]^2+(1+i)(w+w'i) \quad \text{d. i.}$$

$$D+D'i \equiv [(1+i)(v+v'i)]^2 \; mod\, 1+i$$

Ist dagegen $D+D'i$ nicht durch $1+i$ theilbar, also von der Form $(1+i)(r+r'i)+1$, und man setzt

$$(1+i)(r+r'i)+1=[(1+i)(v+v'i)+1]^2+y+y'i$$

so wird offenbar ebenfalls $y+y'i$ durch $1+i$ theilbar oder $=(1+i)(w+w'i)$ sein, woraus derselbe obige Schluss folgt.

V. Wenn $q+q'i=(1+i)^2=2i$ ist; so sind unter allen zu $q+q'i$ relativ primen Werthen von $D+D'i$, welche offenbar entweder die Form $2r+1+2r'i$ oder die Form $2r+(2r'+1)i$ haben, die ersteren quadratische Reste, die letzteren dagegen quadratische Nichtreste nach $q+q'i$.

Denn hat $D+D'i$ die Form $2r+1+2r'i$, und setzt man

$$2r+1+2r'i=[2(v+v'i)+1]^2+y+y'i$$

worin $v+v'i$ willkürlich ist; so ist $y+y'i$ von der Form $2w+2w'i=2(w+w'i)=(1+i)^2(w'-wi)$, also

$$2r+1+2r'i=[2(v+v'i)+1]^2+(1+i)^2(w'-wi) \text{ d. i.}$$

$$D+D'i\equiv[2(v+v'i)+1]^2 \mod (1+i)^2$$

Hat dagegen $D+D'i$ die Form $2r+(2r'+1)i$, und wäre es möglich, dass $D+D'i\equiv(x+x'i)^2 \mod (1+i)^2$ sei; so müsste in der Gleichung

$$2r+(2r'+1)i=(x+x'i)^2+y+y'i$$

das Glied $y+y'i$ durch $(1+i)^2$ theilbar, also vollkommen paar sein. Dies ist unmöglich; denn wäre es der Fall; so kann offenbar $x+x'i$ nicht durch $1+i$ theilbar sein, weil die linke Seite $D+D'i$ es nicht ist. Es ist also $x+x'i$ entweder unvollkommen paar oder unvollkommen unpaar, mithin $(x+x'i)^2$ unvollkommen unpaar, d. i. $=2v+1+2v'i$. Demnach ist

$$y+y'i=2r-v-1+(2r'-2v'+1)i$$

$$=2w+1+(2w'+1)i$$

also vollkommen unpaar, mithin nicht durch $(1+i)^2=2i$ theilbar. Es kann also keine Zahl von der Form $D+D'i=2r+(2r'+1)i$ ein quadratischer Rest nach $(1+i)^2$ sein.

VI. Wenn $q+q'i=(1+i)^3=2(1+i)i$ ist; so sind unter allen zu $q+q'i$ relativ primen Werthen von $D+D'i$, welche offenbar entweder die Form $2r+1+2r'i$ oder die Form $2r+(2r'+1)i$ haben, zuvörderst die letzteren sämmtlich quadratische Nichtreste nach $q+q'i$, wie schon aus dem vorhergehenden Satze erhellet, indem dieselben danach keine quadratischen Reste nach $(1+i)^2$ sein können.

Von den ersteren Zahlen der Form $2r+1+2r'i$ aber sind nur die in den Formen $4r+1+4r'i$ und $4r+3+(4r'+2)i$ enthaltenen quadratische Reste, dagegen die in den Formen $4r+1+(4r'+2)i$ und $4r+3+4r'i$ enthaltenen quadratische Nichtreste nach $q+q'i$.

Denn substituirt man in der Gleichung

$$D+D'i=(x+x'i)^2+y+y'i$$

worin nach der obigen Bemerkung $(x+x'i)^2$ nur die Form $2v+1+2v'i$ haben kann, für $D+D'i$ nach und nach jede einzelne der genannten Formen und beachtet, dass $y+y'i=(1+i)^3(u+u'i)2(1+i)(t+t'i)$ sein soll; so findet man, dass Dies nur in folgenden beiden Fällen denkbar ist. Nämlich wenn man $D+D'i=4r+1+4r'i$ hat, indem dann

$$y+y'i=4w+4w'i=4(w+w'i)=-(1+i)^4(w+w'i)$$

wird, oder wenn man $D+D'i=4r+3+(4r'+2)i$ hat, indem dann

$$y+y'i=4w+2+(4w'+2)i=i^3(1+i)^2[w+w'+1+(w'-w)i]$$

wird. Im ersteren dieser eben bezeichneten beiden möglichen

Fälle ist also $y+y'i$ nicht bloss durch $q+q'i=(1+i)^3$, sondern auch durch $(1+i)^4$ theilbar; im letzteren jedoch nur durch $q+q'i=(1+i)^3$ und nicht durch $(1+i)^4$, indem der Faktor $w+w'+1+(w'-w)i$ durchaus entweder die Form $2t+(2t'+1)i$ oder die Form $2t+1+2t'i$ besitzt, also den Faktor $1+i$ nicht enthält.

VII. Wenn $q+q'i=(1+i)^4=-4$ ist; so leuchtet zuvörderst ein, dass alle Werthe $D+D'i$, welche nicht quadratische Reste nach $(1+i)^3$ sein können, Dies auch nicht nach $(1+i)^4$ zu sein vermögen. Es kommen also nur noch die Werthe von $D+D'i$ in Betracht, welche die Form $4r+1+4r'i$ und $4r+3+(4r'+2)i$ besitzen. Hiervon sind die ersteren quadratische Reste, die letzteren dagegen quadratische Nichtreste nach $q+q'i$.

Die Richtigkeit dieses Satzes leuchtet aus der Schlussbemerkung des vorhergehenden Satzes ein.

VIII. Wenn $q+q'i=(1+i)^n$ und $n>4$ ist; so kommen nur noch diejenigen Werthe von $D+D'i$ in Betracht, welche nach dem vorhergehenden Satze quadratische Reste nach $(1+i)^4$ sind, also die Werthe von der Form $4r+1+4r'i$. Hiervon sind die in den Formen $8r+1+8r'i$ und $8r+5+(8r'+4)i$ enthaltenen Werthe quadratische Reste, alle übrigen aber quadratische Nichtreste nach $q+q'i$.

Zuerst beweisen wir diesen Satz für $n=5$, also für $q+q'i=(1+i)^5=-4(1+i)$. Setzt man zu diesem Ende

$$D+D'i=4r+1+4r'i=(x+x'i)^2+y+y'i$$

und beachtet, dass $(x+x'i)^2$ als Quadrat einer unvollkommen paaren oder unpaaren Zahl stets unvollkommen unpaar und zwar resp. von der Form

$$[2v+(2v'+1)i]^2=4v^2-4v'^2-4v'-1+(8vv'+4v)i$$

oder von der Form

$$[2v+1+2v'i]^2=4v^2-4v'^2+4v+1+(8vv'+4v')i$$

ist; so erhält man bei Zugrundelegung der ersten Form

$$y+y'i=4r-4v^2+4v'^2+4v'+2+(4r'-8vv'-4v)i$$

und bei Zugrundelegung der zweiten Form

$$y+y'i=4r-4v^2+4v'^2-4v+(4r'-8vv'-4v')i$$

Der erste Werth von $y+y'i$ ist nicht durch 4, also auch nicht durch $(1+i)^5=-4(1+i)$ theilbar, und ist demnach ausser Acht zu lassen.

Damit aber der zweite Werth durch $4(1+i)$ theilbar werde, muss

$$\frac{y+y'i}{4}=r-v^2+v'^2-v+(r'-2vv'-v')i$$

noch durch $1+i$ theilbar, also entweder vollkommen paar oder vollkommen unpaar sein. Da unter allen Umständen v^2+v und $2vv'$ paare Zahlen sind; so kommt es nur darauf an, ob

$$r+v'^2+(r'-v')i$$

vollkommen paar oder vollkommen unpaar werden kann. Dies ist allerdings möglich, jedoch nur dann, wenn r und r' entweder gleichzeitig paar oder gleichzeitig unpaar sind, also nur dann, wenn $D+D'i$ entweder die Form $8r+1+8r'i$ oder die Form $8r+5+(8r'+4)i$ hat.

Hierdurch ist der obige Satz für $n=5$ erwiesen.

Was den allgemeinen Fall $n>5$ betrifft; so sei für irgend einen Werth n, welcher >4 ist,

$$D+D'i\equiv(x+x'i)^2 \; mod\,(1+i)^n \quad \text{also}$$
$$D+D'i-(x+x'i)^2=(v+v'i)(1+i)^n$$

Ist nun $w+w'i$ eine beliebige ganze Zahl; so hat man

$$D+D'i-[x+x'i+(w+w'i)(1+i)^{n-2}]^2$$
$$=D+D'i-(x+x'i)^2+(w+w'i)(x+x'i)i(1+i)^n$$
$$+(w+w'i)^2(1+i)^{2n-4}$$
$$=(v+v'i)(1+i)^n+(w+w'i)(x+x'i)i(1+i)^n+(w+w'i)^2(1+i)^{2n-4}$$
$$=[v+v'i+(w+w'i)(x+x'i)i+(w+w'i)^2(1+i)^{n-4}](1+i)^n$$

Weil aber $x+x'i$ relativ prim zu $1+i$ ist; so kann die Willkürliche $w+w'i$ stets so bestimmt werden, dass $v+v'i+(w+w'i)(x+x'i)i$ ein Vielfaches von $1+i$, also $=(u+u'i)(1+i)$ wird, indem Dies nur die Auflösung der stets möglichen diophantischen Gleichung vom ersten Grade

$$(u+u'i)(1+i)-(w+w'i)(x+x'i)i=v+v'i$$

für die beiden Unbekannten $u+u'i$ und $w+w'i$ erfordert. Für einen solchen Werth von $w+w'i$ wird aber die rechte Seite der vorstehenden Gleichung

$$=[(u+u'i)(1+i)+(w+w'i)^2(1+i)^{n-4}](1+i)^n$$

und wenn $n>4$ ist, kann man in der vorderen Klammer nochmals den Faktor $1+i$ absondern, wodurch jener Ausdruck

$$=[u+u'i+(w+w'i)^2(1+i)^{n-5}](1+i)^{n+1}$$

wird.

Hierdurch ist gezeigt, dass wenn $D+D'i$ quadratischer Rest nach $(1+i)^n$ und $n>4$ ist, es auch stets quadratischer Rest nach $(1+i)^{n+1}$ sein wird. Demnach sind die vorhin be-

zeichneten Werthe von $D+D'i$, welche quadratische Reste nach $(1+i)^5$ sind, auch quadratische Reste nach jeder höheren Potenz von $1+i$.

C. Wenn $q+q'i$ die Potenz einer in $D+D'i$ aufgehenden Primzahl ist.

IX. Wenn $q+q'i$ in $D+D'i$ aufgeht; so ist $D+D'i$ stets ein quadratischer Rest nach $q+q'i$, welchen Werth auch die letztere Zahl haben möge.

X. Wenn $q+q'i$ in $D+D'i$ nicht aufgeht, aber die Potenz einer in $D+D'i$ aufgehenden Primzahl $r+r'i$ (welche auch $=1+i$ sein kann) darstellt, wenn man also $q+q'i=(r+r'i)^m$ und $D+D'i=(r+r'i)^n(E+E'i)$ hat, worin $m>n$ ist, und der Faktor $E+E'i$ die Primzahl $r+r'i$ nicht weiter enthält; so ist $D+D'i$ ein quadratischer Nichtrest nach $q+q'i$, wenn n einen unpaaren Werth hat.

XI. Hat dagegen für die vorstehende Voraussetzung n einen paaren Werth; so ist $D+D'i$ ein quadratischer Rest oder Nichtrest nach $q+q'i$, jenachdem $E+E'i$ ein quadratischer Rest oder Nichtrest nach $r+r'i$ ist.

Die vorstehenden Sätze sind wie in §. 150, C. zu beweisen.

D. Allgemeinster Fall, wo $q+q'i$ in beliebiger Weise zusammengesetzt ist.

XII. Ist endlich $q+q'i$ das Produkt aus Potenzen beliebiger Primzahlen, also $=(r+r'i)^m(s+s'i)^n\ldots$; so ist hier, wie in §. 150, X., $D+D'i$ dann und auch nur dann quadratischer Rest nach $q+q'i$, wenn es ein solcher nach jeder der Zahlen $(r+r'i)^m$, $(s+s'i)^n\ldots$ ist, auf welche Eigenschaft $D+D'i$ nach den vorstehenden Sätzen stets geprüft werden kann.

XIII. Endlich gelten auch hier die Sätze des §. 150 sub XI. bis XIII.

§. 216. *Ausdehnung der übrigen Gesetze des sechsten Abschnittes auf die komplexen Zahlen.*

I. Was die übrigen im sechsten Abschnitte für reelle Zahlen ermittelten Gesetze betrifft; so lassen sich die meisten derselben mit Leichtigkeit auch für komplexe Zahlen erweitern. Man hat dann, wo dort schlechthin von Primzahlen die Rede

war, jetzt vollkommene Primzahlen zu verstehen. Statt der dortigen Zahlen, welche relativ prim zu einer gegebenen Zahl q und kleiner als dieselbe sind, hat man jetzt diejenigen Zahlen zu nehmen, welche relativ prim zu $q+q'i$ sind und in einem der mehr erwähnten Quadrate liegen, dessen Seite durch die (reelle oder komplexe) Zahl $q+q'i$ dargestellt wird. Ausserdem ist an den Stellen, wo dort die paare Primzahl 2 von den unpaaren Primzahlen unterschieden werden musste, jetzt die Primzahl $1+i$ mit paarer Norm von den Primzahlen mit unpaarer Norm zu unterscheiden.

II. Hiernach erkennt man zuvörderst, dass auch für komplexe Zahlen die Gesetze des §. 151 hinsichtlich der Faktoren Gültigkeit behalten, aus denen quadratische Reste oder *Nichtreste* zusammengesetzt sind.

III. Ferner gelten die Sätze des §. 152 von IV. bis VII. über die Anzahl der Wurzeln einer reinen quadratischen Kongruenz für die Fälle, wo der Model von unpaarer Norm und relativ prim zu D ist. Die Bestimmung dieser Anzahl für die übrigen Fälle müssen wir, um dieses Werk nicht zu sehr auszudehnen, dem Leser überlassen.

IV. Die Untersuchung des §. 153 über die lineare Form der Primfaktoren von $D-x^2$ lässt sich auch auf komplexe Zahlen ausdehnen. Das Prinzip bleibt dem früheren gleich, die Spezialisirungen würden jedoch hier zu weit führen.

V. Die in §. 154 sub I. und III. bis VII. mitgetheilten Sätze über die Eigenschaften der Zahlen von der Form x^2-Dy^2 gelten auch für komplexe Zahlen.

Was jedoch die reduzirten quadratischen Formen in komplexen Zahlen betrifft; so sind die Regeln für deren Darstellung aus §. 201 und 205 zu entnehmen. Wenn nämlich P^n den absoluten Werth des halben mittleren Koeffizienten (welcher bekanntlich immer als vollständig paar vorausgesetzt wird) Q_n, Q_{n-1} die absoluten Werthe der beiden äusseren Koeffizienten und D den absoluten Werth der Determinante der quadratischen Form bezeichnen; so kann man für den Fall, dass die Determinante kein Quadrat ist, nach §. 201 stets bewirken, dass P^n sowol $\leqq Q_n\sqrt{\frac{1}{2}}$, als auch $\leqq Q_{n-1}\sqrt{\frac{1}{2}}$, ferner dass $P_n\leqq\sqrt{D}$ und dass entweder Q_n oder $Q_{n-1}<D$ und nur wenn $D=1$ ist, $=D$ wird.

Für den Fall aber, dass die Determinante ein **Quadrat** d^2 ist, lässt sich nach §. 205 stets $P_n = d$, $Q_n = 0$ und $Q_{n-1} \leqq \sqrt{2d}$ machen.

Durch diese allgemeineren Beziehungen, wodurch auch der Unterschied zwischen positiven und negativen Determinanten aufgehoben wird, ändern sich für komplexe Zahlen in mehrfacher Weise die speziellen Resultate in §. 154 sub VIII. bis XV.

VI. Hierauf kann man nach den Prinzipien des §. 155 die lineare Form der durch quadratische Formen dargestellten Primzahlen bestimmen.

Die Spezialisirung dieser Aufgabe wird übrigens bei Zulassung komplexer Zahlen die Resultate des §. 156 wesentlich ändern.

So verliert z. B. der von Fermat für reelle Zahlen gefundene Satz in §. 156, I, wonach jede Primzahl von der Form $4n+1$ sich auf einzige Weise, jede Primzahl von der Form $4n+3$ aber gar nicht in zwei Quadrate zerlegen lasse, bei der Zuziehung von komplexen Zahlen nicht bloss seine Bedeutung, weil bekanntlich reelle Zahlen von der Form $4n+1$ gar keine vollkommenen Primzahlen sind, sondern auch seine Gültigkeit, indem sich jede reelle Primzahl von der Form $4n+1$ auf mehrfache Weise in zwei Quadrate zerlegen lässt (z. B. $13 = 3^2 + 2^2 = 7^2 + (6i)^2$), und ausserdem jede reelle Primzahl von der Form $4n+3$ sehr wohl als Summe zweier Quadrate darstellbar ist (z. B. $7 = 4^2 + (3i)^2$).

Man hat vielmehr folgende allgemeine Sätze. Jede unvollständig unpaare Primzahl ist in der Form x^2+y^2, nicht aber in der Form $(x^2+y^2)i$ enthalten, und zwar nur auf eine einzige Weise, wenn man die negativen Werthe von x und y als gleichbedeutend mit den positiven ansieht. Jede unvollständig paare Primzahl ist in der Form $(x^2+y^2)i$, nicht aber in der Form x^2+y^2 enthalten, und zwar nur auf eine einzige Weise. Eine vollständig unpaare Primzahl oder Eine von der paaren Norm 2, also $\pm(1+i)$ oder $\pm(1-i)$ ist weder in der Form x^2+y^2, noch in der Form $(x^2+y^2)i$ darstellbar. Das Letztere gilt überhaupt von jeder vollkommen unpaaren Zahl; und was die übrigen zusammengesetzten Zahlen betrifft; so gestatten sie mit Ausnahme der Zahl ± 2 oder $\pm 2i$, welche nur einzig in der Form x^2+y^2 resp. $(x^2+y^2)i$ darstellbar ist, stets eine mehrfache Darstellung in der Form x^2+y^2 oder $(x^2+y^2)i$ oder in beiden zugleich.

Hiernach ist es ein ausschliessliches Merkmal der vollkommenen Primzahlen von unpaarer Norm

und der Zahlen vom absoluten Werthe 2, dass sie sich auf eine einzige Weise in der Form x^2+y^2, resp. $(x^2+y^2)i$ darstellen lassen.

VII. Schliesslich bemerken wir, dass es keine Schwierigkeiten hat, die Betrachtungen der §§. 157 bis 159 über die Kongruenzen höherer Grade auch für komplexe Zahlen zu erweitern.

Tafel
der
primitiven Wurzeln der Kongruenzen.

Model p	Exponent n	Primitive Wurzeln der Kongruenz $x^n \equiv 1$
3	2	2
5	2	4
	4	2.3
7	2	6
	3	2.4
	6	3.5
11	2	10
	5	3.4.5.9
	10	2.6.7.8
13	2	12
	3	3.9
	4	5.8
	6	4.10
	12	2.6.7.11
17	2	16
	4	4.13
	8	2.8.9.15
	16	3.5.6.7.10.11.12.14
19	2	18
	3	7.11
	6	8.12
	9	4.5.6.9.16.17
	18	2.3.10.13.14.15
23	2	22
	11	2.3.4.6.8.9.12.13.16. 18
	22	5.7.10.11.14.15.17. 19.20.21
29	2	28
	4	12.17
	7	7.16.20.23.24.25.
	14	4.5.6.9.13.22
	28	2.3.8.10.11.14.15. 18.19.21.26.27
31	2	30
	3	5.25
	5	2.4.8.16
	6	6.26
	10	15.23.27.29
	15	7.9.10.14.18.19.20. 28
	30	3.11.12.13.17.21.22. 24.
37	2	36
	3	10.26
	4	6.31
	6	11.27
	9	7.9.12.16.33.34
	12	8.14.23.29
	18	3.4.21.25.28.30.
	36	2.5.13.15.17.18.19. 20.22.24.32.35
41	2	40
	4	9.32
	5	10.16.18.37
	8	3.14.27.38
	10	4.23.25.31
	20	2.5.8.20.21.33.36.39
	40	6.7.11.12.13.15.17. 19.22.24.26.28.29. 30.34.35

Model p	Exponent n	Primitive Wurzeln der Kongruenz $x^n \equiv 1$
43	2	42
	3	6.36
	6	7.37
	7	4.11.16.21.35.41
	14	2.8.22.27.32.39
	21	9.10.13.14.15.17.23.24.25.31.38.40
	42	3.5.12.18.19.20.26.28.29.30.33.34
47	2	46
	23	2.3.4.6.7.8.9.12.14.16.17.18.21.24.25.27.28.32.34.36.37.42
	46	5.10.11.13.15.19.20.22.23.26.29.30.31.33.35.38.39.40.41.43.44.45.
53	2	52
	4	23.30
	13	10.13.15.16.24.28.36.42.44.46.47.49.
	26	4.6.7.9.11.17.25.29.37.38.40.43
	52	2.3.5.8.12.14.18.19.20.21.22.26.27.31.32.33.34.35.39.41.45.48.50.51
59	2	58
	29	3.4.5.7.9.12.15.16.17.19.20.21.22.25.26.27.28.29.35.36.41.45.46.48.49.51.53.57
	58	2.6.8.10.11.13.14.18.23.24.30.31.32.33.34.37.38.39.40.42.43.44.47.50.52.54.55.56
61	2	60
	3	13.47
	4	11.50
	5	9.20.34.58
	6	14.48
	10	3.27.41.52
	12	21.29.32.40
	15	12.15.16.22.25.42.56.57
	20	8.23.24.28.33.37.38.53
	30	4.5.19.36.39.45.46.49
	60	2.6.7.10.17.18.26.30.31.35.43.44.51.54.55.59
67	2	66
	3	29.37
	6	15.22.30.38
	11	9.14.24.25.40.59.62.64
	22	3.5.8.27.42.43.45.52.53.58
	33	4.6.10.16.17.19.21.23.26.33.35.36.39.47.49.54.55.56.60.65
	66	2.7.11.12.13.18.20.28.31.32.34.41.44.46.48.50.51.57.61.63

Tafel der Indizes.

Modul p	Basis B	Indizes der Zahlen 2. 3. 5. 7.11.	13.17.19.23.29.	31.37.41.43.47.
3	2	1.		
5	2	1. 3.		
7	3	2. 1. 5.		
11	2	1. 8. 4. 7.		
13	6	5. 8. 9. 7.11.		
17	10	10.11. 7. 9.13.	12.	
19	10	17. 5. 2.12. 6.	13. 8.	
23	10	8.20.15.21. 3.	12.17. 5.	
29	10	11.27.18.20.23.	2. 7.15.24.	
31	17	12.13.20. 4.29.	23. 1.22.21.27.	
37	5	11.34. 1.28. 6.	13. 5.25.21.15.	27.
41	6	26.15.22.39. 3.	31.33. 9.36. 7.	28.32.
43	28	39.17. 5. 7. 6.	40.16.29.20.25.	32.35.18.
47	10	30.18.17.38.27.	3.42.29.39.43.	5.24.25.37.
53	26	25. 9.31.38.46.	28.42.41.39. 6.	45.22.33.30.8.

Modul p	Basis B	Indizes der Zahlen 2. 3. 5. 7.11. 13.17.19.23.29. 31.37.41.43.47. 53.59.61.67.71. 73.79.83.89.
59	10	25.32.34.44.45. 23.14.22.27. 4. 7.41. 2.13.53. 28.
61	10	47.42.14.23.45. 20.49.22.39.25. 13.33.18.41.40. 51.17.
67	12	29. 9.39. 7.61. 23. 8.26.20.22. 43.44.19.63.64. 3.54. 5.
71	62	58.18.14.33.43. 27. 7.38. 5. 4. 13.30.55.44.17. 59.29.37.11.
73	5	8. 6. 1.33.55. 59.21.62.46.35. 11.64. 4.51.31. 53. 5.58.50.44.
79	29	50.71.34.19.70. 74. 9.10.52. 1. 76.23.21.47.55. 7.17.75.54.33. 4.
83	50	3.52.81.24.72. 67. 4.59.16.36. 32.60.38.49.69. 13.20.34.53.17. 43.47.
89	30	72.87.18. 7. 4. 65.82.53.81.29. 57.77.67.59.34. 10.45.19.32.26. 68.46.27.
97	10	86. 2.11.53.82. 83.19.27.79.47. 26.41.71.44.60. 14.65.32.51.25. 10.42.91.18.

Tafel
der vollkommenen Primzahlen
$a + bi$
bis zur Norm $a^2 + b^2 = 4001$.

Norm a^2+b^2	Absoluter Werth von a und b oder b und a		Norm a^2+b^2	Absoluter Werth von a und b oder b und a		Norm a^2+b^2	Absoluter Werth von a und b oder b und a		Norm a^2+b^2	Absoluter Werth von a und b oder b und a	
1	1	0	281	16	5	673	23	12	1097	29	16
2	1	1	293	17	2	677	26	1	1109	25	22
5	2	1	313	13	12	701	26	5	1117	26	21
9	3	0	317	14	11	709	22	15	1129	27	20
13	3	2	337	16	9	733	27	2	1153	33	8
17	4	1	349	18	5	757	26	9	1181	34	5
29	5	2	353	17	8	761	20	19	1193	32	13
37	6	1	361	19	0	769	25	12	1201	25	24
41	5	4	373	18	7	773	22	17	1213	27	22
49	7	0	389	17	10	797	26	11	1217	31	16
53	7	2	397	19	6	809	28	5	1229	35	2
61	6	5	401	20	1	821	25	14	1237	34	9
73	8	3	409	20	3	829	27	10	1249	32	15
89	8	5	421	15	14	853	23	18	1277	34	11
97	9	4	433	17	12	857	29	4	1289	35	8
101	10	1	449	20	7	877	29	6	1297	36	1
109	10	3	457	21	4	881	25	16	1301	26	25
113	8	7	461	19	10	929	23	20	1321	36	5
121	11	0	509	22	5	937	24	19	1361	31	20
137	11	4	521	20	11	941	29	10	1373	37	2
149	10	7	529	23	0	953	28	13	1381	34	15
157	11	6	541	21	10	961	31	0	1409	28	25
173	13	2	557	19	14	977	31	4	1429	30	23
181	10	9	569	20	13	997	31	6	1433	37	8
193	12	7	577	24	1	1009	28	15	1453	38	3
197	14	1	593	23	8	1013	23	22	1481	35	16
229	15	2	601	24	5	1021	30	11	1489	33	20
233	13	8	613	18	17	1033	32	3	1493	38	7
241	15	4	617	19	16	1049	32	5	1549	35	18
257	16	1	641	25	4	1061	31	10	1553	32	23
269	13	10	653	22	13	1069	30	13	1597	34	21
277	14	9	661	25	6	1093	33	2	1601	40	1

Norm a^2+b^2	Absoluter Werth von a und b oder b und a		Norm a^2+b^2	Absoluter Werth von a und b oder b und a		Norm a^2+b^2	Absoluter Werth von a und b oder b und a		Norm a^2+b^2	Absoluter Werth von a und b oder b und a	
1609	40	3	2161	44	15	2753	52	7	3433	52	27
1613	38	13	2209	47	0	2777	44	29	3449	43	40
1621	39	10	2213	47	2	2789	50	17	3457	44	39
1637	31	26	2221	45	14	2797	51	14	3461	50	31
1657	36	19	2237	46	11	2801	49	20	3469	45	38
1669	38	15	2269	37	30	2833	48	23	3481	59	0
1693	37	18	2273	47	8	2837	41	34	3517	59	6
1697	41	4	2281	45	16	2857	51	16	3529	48	35
1709	35	22	2293	42	23	2861	50	19	3533	58	13
1721	40	11	2297	44	19	2897	44	31	3541	54	25
1733	38	17	2309	47	10	2909	53	10	3557	49	34
1741	30	29	2333	43	22	2917	54	1	3581	59	10
1753	32	27	2341	46	15	2953	53	12	3593	53	28
1777	39	16	2357	41	26	2957	46	29	3613	43	42
1789	42	5	2377	44	21	2969	40	37	3617	44	41
1801	35	24	2381	35	34	3001	51	20	3637	46	39
1849	43	0	2389	42	25	3037	54	11	3673	48	37
1861	31	30	2393	37	32	3041	55	4	3677	59	14
1873	33	28	2417	49	4	3049	45	32	3697	49	36
1877	41	14	2437	49	6	3061	55	6	3701	55	26
1889	40	17	2441	40	29	3089	55	8	3709	53	30
1901	35	26	2473	48	13	3109	47	30	3733	57	22
1913	43	8	2477	46	19	3121	40	39	3761	56	25
1933	42	13	2521	36	35	3137	56	1	3769	60	13
1949	43	10	2549	50	7	3169	55	12	3793	52	33
1973	38	23	2557	46	21	3181	45	34	3797	46	41
1993	43	12	2593	48	17	3209	53	20	3821	61	10
1997	34	29	2609	47	20	3217	56	9	3833	53	32
2017	44	9	2617	51	4	3221	55	14	3853	62	3
2029	45	2	2621	50	11	3229	50	27	3877	54	31
2053	42	17	2633	43	28	3253	57	2	3881	59	20
2069	38	25	2657	49	16	3257	56	11	3889	60	17
2081	41	20	2677	39	34	3301	49	30	3917	61	14
2089	45	8	2689	40	33	3313	57	8	3929	52	35
2113	33	32	2693	47	22	3329	52	25	3989	58	25
2129	40	23	2713	52	3	3361	56	15	4001	49	40
2137	36	29	2729	52	5	3373	58	3			
2141	46	5	2741	46	25	3389	58	5			
2153	37	28	2749	43	30	3413	58	7			